＜平成２５年度修士論文（静岡文化芸術大学大学院文化政策研究科）＞

サイバー攻撃に対処する国家ネットワークセキュリティの構築

Construction of a national information security system against cyber-attacks.

齋藤　亜紀　Aki Saito

（論文指導：静岡文化芸術大学教授　藤田憲一）

目　　次

論文要旨

本論文は近年頻発しているサイバー攻撃の脅威に対し、日本の情報セキュリティの在り方に問題意識を持ち、日本における国家的な情報セキュリティ向上のための方策を考察したものである。

サイバー攻撃は新しい脅威である。しかし、標的になっているネットワークやシステムのセキュリティだけでなく、そのネットワークを運用する人間的側面のセキュリティも向上させる必要がある。人間的側面のセキュリティとは法的規制や制度、セキュリティ組織の設立、軍隊のサイバー部門の強化などを指す。

そこで、未だ共通の定義がないサイバー攻撃についてその概念の整理を試み、現段階での人間的セキュリティの現状を検討する。

それらの考察から分かったことは、サイバー攻撃に対して国際社会も日本も法的規制や情報セキュリティが不十分であり、その攻撃の特徴から今後もサイバー攻撃を規制しうる実効的な対抗策を編み出すことは難しいということである。つまりサイバー攻撃への対処は対象となりうる組織が自発的にセキュリティ向上に努めなければならず、まずセキュリティ構築は民間レベルで行うべきであると考えられる。だが利益を見出しにくいセキュリティ人材は企業において軽視される傾向があるため、政府は企業などに対し情報セキュリティの「抜き打ち検査」を行い、重大な欠陥を発見した場合にペナルティを課すことが有効であると考えられる。その一方で政府は第 3 者機関に監査を依頼し、自らの情報セキュリティも向上させるべきである。

そのための人材育成として、政府は情報セキュリティ企業に出資することによって人材の増加を狙う。その上で、政府は外交を通じて情報交換を積極的に行うべきである。だが利害関係が対立する 2 国間では難しいため、情報交換や議論は国連などの多国間での場が相応しいだろう。また多国間のサイバー攻撃に関する研究機関を運営し、その技術を民間と共有することも政府の役割として重要である。

キーワード　：　サイバー攻撃　サイバー犯罪　サイバー戦争　情報セキュリティ政策

Abstract

In this thesis, I have examined measures to strengthen information security in Japan, against the threat of frequent cyber-attacks.

To defend against the threat of cyber-attacks, it is necessary to improve not only security networks and systems themselves but also security of human dimensions—such as legal regulations, social institutions, Information organization, and military cyber units among other things.

In examining security systems of human dimensions in Japan and the international community, I found that security is not still adequate and that it is difficult to develop effective countermeasures, which can defend against cyber-attacks.

Therefore, it seems the most realistic approach would be for the private sector to take the initiative in efforts to strengthen information security systems and have the government support their efforts. On the other hand, the government should improve their own security based on input from third party evaluation.

To develop human resources for information security, the government should make surprise inspections and support IT companies financially. The government should also actively exchange information concerning cyber-attacks through diplomatic channels either bilaterally or multilaterally (i.e. via the United Nations), create research organizations with other countries and share security technologies with the private sector.

はじめに

通信技術の飛躍的な進歩とコンピュータや携帯電話の普及に伴って情報化社会は急速に成長し、我々は様々な利便性を手に入れた。インターネットで買い物をする、電車の自動改札口を通る、メールを送受信する、というような行為はすべて情報化社会が可能にした行動である。このような情報システムは社会の様々な場面で活用されており、我々の生活にとって必要不可欠な存在になっている。

だが、その一方で情報化社会は新たな危険性を生み出した。それはコンピュータ犯罪や個人情報の漏洩、プライバシーの問題などである。その中でも近年最も危険性が高いと注目されているのが「サイバー攻撃」である。サイバー攻撃とは、コンピュータ・システムやインターネットなどを利用して、標的のコンピュータやネットワークに不正に侵入してデータの詐取や破壊、改ざんなどを行なったり、標的のシステムを機能不全に陥らせることを指す。その攻撃対象は金融システムや交通システム、電力供給システムなど多岐に渡り、我々の生活と密接なシステムが危険にさらされている。そのような危険に直面し、国際社会はサイバー攻撃を重大な脅威として認識し始め各国が競って対処しようとしている。

アメリカは2010年に「サイバー軍(USCYBERCOM)」を設置し、翌年7月サイバー空間における防衛はこれまでの海、陸、空、宇宙に続く「新たな戦争の場」と認識し、サイバー攻撃に対して国家をあげて立ち向うという意志があることを宣言した。一方日本も、2013年度末にサイバー攻撃に対処する「サイバー防衛隊」を陸海空の3自衛隊を集約して約90人で発足する予定であり、防衛省は今年度予算にサイバー関連経費約140億円を計上した。このようにサイバー攻撃は国際社会にとって安全保障を脅かす重大な脅威として認識され、様々な対応がとられている。

だが、未だ国際社会は「サイバー攻撃」を明確に定義しておらず、それらの議論が不十分のままメディアなどを通じてその言葉が一人歩きをしている。時折サイバー攻撃は核爆弾にも匹敵する脅威と言われているが、本当にメディアで語られているほどの危険性を有しているのだろうか。我々は誇張されているサイバー攻撃の脅威に対して対策を講じたり議論したりするのではなく、実際に起きているサイバー攻撃に即した政策が必要である。

本研究はそのような問題意識を出発点とし、日本の情報セキュリティの在り方を考察する。情報セキュリティにおいて技術的な改善や強化はもちろん重要であるが、その一方で事務的セキュリティやサイバー攻撃に対する法的規制、セキュリティ向上・維持のための制度、セキュリティ組織の設立、軍隊のサイバー部門の強化というような側面も改善する必要がある。

本論文の目的は、サイバー攻撃から国民の生活を守るために政府はどのような国家ネットワークセキュリティを構築するべきなのか考察する。

第1章　サイバー攻撃とは

サイバー攻撃とは一体何だろうか。最近になって政府や企業がサイバー攻撃の被害に遭っているが、個人が直接的にサイバー攻撃の被害に遭うことはほとんどない。舞台となるのがネットワークの世界であるため、サイバー攻撃を行っている犯人の顔はわからないし、その被害もどのような損害を被ったのか分かりにくい。インターネットやコンピュータに詳しくない人にとって、その実情は不明な部分が多い。ここではサイバー攻撃の基本的な概要について述べ、次章へのステップとする。

この章では、まずサイバー攻撃の定義について考察する。現段階のメディアや政府の見解では、「サイバー攻撃」が含む範囲を明確にしないまま用語が使用されているが、そのままでは国家的なセキュリティ構築の議論にも支障をきたすため、第1節でその定義を明確にする。

続いて第2節でサイバー攻撃の特徴について述べる。サイバー攻撃は従来の犯罪や武力攻撃とは一線を画するものである。サイバー攻撃を構成する要素「主体」、「目的」、「手法」、「場」、「攻撃対象」を分析し、従来の武力攻撃とは一体何が異なるのかを考察する。

第1節　定義

サイバー犯罪（Cyber-crime）、サイバー攻撃

（Cyber-attack）、サイバー戦争（Cyber-warfare）[1]はそれぞれ普遍的に認知された定義がないので、混合されたままメディアなどで使用される場合がある。しかし、上記 3 つの用語はそれぞれ異なった概念を持っている。共有定義の欠如は重要な法的提案や政策提起にあたって支障があり混乱を招きかねないため、ここでは Hathaway（2012, pp.822-837）らによるサイバー犯罪、サイバー攻撃、サイバー戦争の定義に基づいて考察し、整理を試みたい。

まず、サイバー諸行為の関係を図にすると図 1 のようになる。サイバー犯罪が大きな円を描き、それと少し重複するようにサイバー攻撃がある。同じようにサイバー犯罪に重複しているが、サイバー攻撃の範囲内にあるのがサイバー戦争である。

サイバー犯罪の典型的な定義は、「コンピュータ、ネットワークまたはハードウェアのデバイスを用いて犯される犯罪」である。サイバー犯罪と分類される行為としては、サイバースパイ活動、インターネット上の詐欺行為、オンラインの著作権侵害、コンピュータでの児童ポルノの保管・共有、コンピュータへの不正アクセス等などであり、コンピュータ・ネットワークを破壊や麻痺させるなどネットワークそのものが攻撃目的でないことがわかる。図 1 で描かれている通り、サイバー空間におけるトラブルの大部分はサイバー犯罪であり、非常に幅広い違法行為が含まれている。サイバー犯罪は他の犯罪と同様に、国家ではなく個人または非国家主体によって行われる犯罪行為であり、その目的は政治的または国家の安全目的ではなく、金銭目的などで行われる。

一方、サイバー攻撃は政治的または国家の安全目的でコンピュータ・ネットワークの機能を攻撃する。ここでの主体は非国家主体・国家主体のどちらでもあり得る。非国家主体がコンピュータ・ネットワークの手段によって違法行為を犯し、コンピュータ・ネットワークを攻撃し、そして政治的または国家の安全目的を持っている場合、図 1 に見られるサイバー犯罪とサイバー攻撃が重複するエリアが生じる。ここのエリアでは、武力攻撃またはサイバー戦争に達する活動のレベルまでは上がらないだろう。サイバー犯罪は非国家主体が行うため、これとまったく同じ行為を犯す国家はこの重複部分には入らない。なぜなら国家が行動すれば、それは必然的に政治的または国家の安全目的を持っているからである。

サイバー戦争は武力衝突の文脈で、既存の武力攻撃と同等の効果をもたらす攻撃と定義される。サイバー戦争はサイバー攻撃も構成しなければならないという点で特徴的である。以上のような特徴を表にするといか表 1 のようになる。

本論文では、以上のような 3 つのサイバー行為の内「サイバー攻撃」ないし「サイバー戦争」を取り上げる。本論文のテーマは国家の安全を脅かすサイバー脅威に対処するためのセキュリティの構築であるため、その脅威となる「サイバー攻撃」ないし「サイバー戦争」に限定する。だがサイバー犯罪を一切含まない厳密な概念としてでなく、関連がある限りでサイバー犯罪も含めて議論していく。

第 2 節　特徴

従来の犯罪や武力攻撃などに対して、サイバー攻撃は一体何が異なるのだろうか。ここでは従来の武力攻撃とは一線を画するサイバー攻撃の様々な特徴について検討していく。

加藤（1993, p.35）によれば、「一般に紛争は、『主体（actor）』、『争点（issue）』、『手段（means）』の 3 つの要素と『場（field）』からなる」。サイバー攻撃が発生する際も、この 4 要素すべてに関係しているため、ここではこれらの要素をベースにサイバー攻撃の特徴を見ていく。ただしサイバー攻撃の場合は両者の争いと言うよりも、その攻撃は一方的なものであるためここでは「争点」ではなく「攻撃者が何のために攻撃するのか」という「目的」に焦点を当てる。また、上記 4 つの要素に加えてサイバー攻撃はその場（サイバー空間）が特殊でありその「攻撃対象」も限定的であるため、そのことについても言及する。

1．主体・目的

ここではサイバー攻撃の「主体」と「目的」について述べる。この 2 つは密接な関係なのでここでまとめて議

[1] サイバーテロ（Cyber-terrorism）という用語も存在し、これはコンピュータ・ネットワークに関わる新しいテロリズムを意味する。サイバー空間で暴力手段を行使するというサイバー攻撃に対する非難の意味合いも含まれるため、ここではその用語は扱わない。

論する。

Global Organized Crime Project は、サイバーテロを技術水準と投入資金によって 4 分類している。本論文ではサイバーテロそのものを扱うわけではないが、この 4 分類はサイバー攻撃にも有効であるため紹介する。その 4 分類は①若年者などのハッカーによる愉快犯的犯罪、②高度な技術を持つハッカー集団による犯罪、③金融機関や産業技術などの社会的価値があると考えられるデータを狙った組織的犯罪、④国家やテロリスト集団による犯罪、である[2]。

また土屋（2013a, p.134）によれば、サイバー攻撃の目的を整理すると以下の 4 つに大別できるとした。①物理的な破壊（ダムの決壊や飛行機の衝突など）、②金銭的な詐取（銀行口座への不正アクセスや証券詐欺など）、③心理的な操作や示威的行為（ウェブの書き換えやサービス障害など）、④秘密裏の工作活動、である。また、サイバー攻撃の主体は国家だけでなく高度な技術があれば非政府組織や個人、テロ集団でも参加することが可能である。

初期のサイバー攻撃は自己顕示欲、見せしめ、嫌がらせ等を目的とした愉快犯による犯行が多かった。1980 年代前半に登場したマルウェア[3]は、単に画面が崩れたりメッセージを残したりするだけなど、パソコンに直接被害を与えるようなものはほとんどなかった。つまり、自分の技術を誇示し相手を驚かせたいという知的好奇心を満たすための悪戯のようなものだった。

その後ネットワークの時代が到来し、2000 年前後になると明確な金銭目的のマルウェアが登場した。金銭や示威を目的とするものが出現し、最近では国家や企業の機密情報等を摂取し、重要なデータやシステムを破壊しようとするものが顕著になりつつある。

最近注目を浴びている主体にハクティビストがある。まず、ハクティビズム（hacktivism）とはハッカーたちの「ハック（hack）」と、積極行動主義ないし政治的行動主義を意味する「アクティビズム（activism）」を掛け合わせた造語である。つまりハクティビストとは、インターネット上でハッキングを通じて政治的・社会的な主張や抗議をする人々のことを指す。言葉そのものは 1995 年頃から使われ始めたが、この言葉が注目を浴びたのは国際的ハクティビスト集団[4]「アノニマス」が登場したからである。

「アノニマス」とは「匿名」という意味をもち、確立された組織ではなくネットの掲示板を介して緩やかにつながる集団である。彼らの起源は日本の画像掲示板「ふたば☆ちゃんねる」を模して誕生したアメリカの画像掲示板「4chan」である。名前欄を空欄のまま書き込むと「アノニマス（名無し）」と表示されることが由来とされている。メンバーは自由なインターネットを支持し、情報の流れを妨げるものに対してあらゆる抗議活動を展開する。その主な方法は攻撃対象へのハッキング、DDoS 攻撃、個人情報や機密情報の不正取得と公開などであるが、時として現実世界で活動することもある。

日本企業に対しては、2011 年 5 月にソニーにサイバー攻撃を仕掛けたことがある。その発端はアメリカ人ハッカーが家庭用ゲーム機「プレイステーション 3」のプログラムのミスを見つけ、ネットで公開したことであった。ソニーはそのハッカーに対して訴訟で対抗しようとした。これにアノニマスは反抗し、ソニーのサーバー[5]に大量にメールを送りつけるなどしてサービスが停止するような妨害攻撃を仕掛け、ソニーがその対応に追われている間にシステムの脆弱性をついたとされている。それらのサイバー攻撃の結果、1 億件以上の個人情報を流出させ、ソニーに総額 140 億円の損失を与えた。

また、サイバー攻撃の主体は匿名的であるという特徴がある。攻撃者は自らの痕跡をネット上から消去することができる。その手段の 1 つに匿名化ソフトがあり、有名なものに「Tor：トーア（The onion router）」がある。このソフトはアメリカ海軍調査研究所が開発し、民間の技術者らが改良した後、ネット上で無料ダウンロードす

[2] 猪口ほか編（2005）p.392

[3] コンピュータ・ウイルスなど不正プログラムの総称。詳しくは「第 2 節 手段」で説明する。

[4] メディアなどにおいてアノニマスを「国際的ハッカー集団」と呼んでいる時もあるが、これは厳密な意味では正しくない。彼らはハッキングに限らずあらゆる手段で「情報の自由」を主張している。実際アノニマスは 2012 年 7 月に日本の「違法ダウンロード罰則化法案」への抗議活動の中で東京・渋谷で「オフ会」を開催し、街の清掃活動を通して法案反対を主張した。「渋谷で「アノニマス」がゴミ拾い　無言の“抗議活動”」『MSN 産経フォト』2012 年 7 月 7 日（http://photo.sankei.jp.msn.com/kodawari/data/2012/07/0707shibuya/）2013 年 12 月 16 日閲覧

[5] ほかのプログラムやコンピュータから要求を受けて処理を実行するプログラムや装置を指し、サーバーに処理要求を出す側をクライアントという。大島・堀本著（2011）p.635

ることができる。この Tor は世界各国の複数のサーバーを経由させ、攻撃元の IP アドレスを辿れなくすることができる。

さらに 2010 年 12 月に三菱重工業がサイバー攻撃を受け、サーバーやパソコンがウイルス感染した事件では、その犯罪の経路や手口・犯人を特定することができずに警視庁公安部は「容疑者不詳」のまま書類を東京地検に送り、不起訴処分となった[6]。この事件ではウイルス入りのメールを社員が開封したことから計 81 台のパソコンがウイルスに感染し、一部が北米など十数か国のサーバーに何度も強制接続され社内文書が流出した。このサーバーを契約した人物は中国に住む中国籍の女性の身分証を管理者側に提出し、またこの攻撃プログラムの一部には中国語が使用されていたことも判明した。しかし、公安部はこの女性について中国当局に照会したが回答はなく、全容を把握することはできなかった。この事件で中国政府が関与したと考えることは早計ではあるが、その可能性が全くない訳ではない。つまり国家が関与した痕跡を残さずに、個人や非国家主体にサイバー攻撃を命じることも考えられる。

このようにネットの世界では自分の痕跡を消すことができるため、攻撃者が誰なのか分からないことが多々ある。これを一般的に「アトリビューション（帰属、属性）問題」と呼んでいる[7]。この「アトリビューション問題」は、今後のサイバー攻撃に対する国際法や自衛権行使を考察する際に非常にややこしくする。

2．手段

近年の代表的なサイバー攻撃の手法には以下のようなものが挙げられる。

（1）DoS 攻撃／DDoS 攻撃

サイバー攻撃の典型的な手法であり、前者を「サービス拒否（DoS : Denial of Services attack）攻撃」、後者を「分散型サービス拒否（DDoS : Distributed Denial of Service）攻撃」と呼ばれている。

DoS 攻撃は特定のウェブサーバーなどに対し、不正なデータや大量のデータを送りつけるなどして、サービス停止に追い込む手法である。その発展型が DDoS 攻撃であり、首謀者はマルウェアを不特定多数のコンピュータに感染させ、感染したコンピュータが特定の日時になると標的となるコンピュータのサーバーなどに一斉にアクセス行為をしたり、大量のデータを送信したりするように設定する。比喩的に述べれば、席数 50 人のレストランに一斉に 5000 人の客が押し寄せ、店頭で各々オーダーを叫んでいる状況に似ている。5000 人の客に対して店側は対応しきれず、レストランとしての機能を停止せざるを得ない。さらに DDoS 攻撃はパソコンの所有者が気づかないまま攻撃に加担してしまい、真の犯人を特定することが非常に困難という特徴がある。

この DDoS 攻撃を使った有名なサイバー事件に、2007 年 4 月に起きたエストニアに対するサイバー攻撃があり、これは世界初のサイバー戦争とも呼ばれている。エストニアは「IT 立国」を国策に掲げて世界初のインターネットによる選挙を実施するなど、国全体の電子化を進めている世界で最も進んだインターネット利用の盛んな国である。エストニアは長くロシアの支配下にあり、ソ連崩壊とともに 1991 年に独立した。独立後のエストニアは民族的な、そして反ロシア的な政策が行われていたためエストニア住民とロシア系住民の間に心理的な軋轢が高まっていた。サイバー攻撃のきっかけは、エストニア首都のタリンにある旧ソ連軍将兵の記念像を移設したことに始まる。ロシアのテレビで記念像移設が報じられると、エストニアの措置に反対する声があがり、ほどなくエストニアに対する DDoS 攻撃が始められた。攻撃は乗っ取られてボットネット[8]化した世界 50 か国以上、約 100 万台のパソコンによって行われ、エストニアに流入した総情報量は、通常時の 400 倍以上であったという。この攻撃によってエストニアの銀行業務をはじめ、国内の各種インターネットサービスはほぼ使用不能となった。エストニアに対する攻撃は、ロシアの関与が疑われたが、ロシア政府は関与を否定している。政府が指示した事実はなく、愛国的な若者たちが勝手にやったのだと弁明し、後にロシアの愛国者グループが関与を認めた。

---

[6]「サイバー攻撃、時効成立へ　中国人の影、解明できず　三菱重事件」『朝日新聞』2013 年 12 月 18 日

[7] 土屋ほか著（2013）p.16

[8] 他人のパソコンの悪用を目的として開発されたプログラムであるボットに感染してしまったゾンビ PC の集合体（乗っ取られた PC の集合体）のこと。また、それらで構成されるネットワークの名称である。大島・堀本著（2011）p.1038

（2）マルウェア

マルウェアとは悪意を持ったソフトウェアの総称である。広義のコンピュータ・ウイルスはこの意味で使用される場合が多い。

経済産業省の「コンピュータウイルス対策基準[9]」では、コンピューターウイルスを次のように定義している。

> 第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、 次の機能を一つ以上有するもの。
> ①自己伝染機能
> 自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能。
> ②潜伏機能
> 発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能。
> ③発病機能
> プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能。

また、ウイルスの種類は以下のようなものがある。

> ・コンピュータ・ウイルス：ネットワークやディスクなどを介して、コンピュータからコンピュータへ勝手にコピー増殖していくようなプログラムのこと。病原体のウイルスが伝染する様に例えて、こう呼ばれている[10]。（狭義のウイルス）
> ・ワーム：ミミズやウジムシのような虫を意味し、転じてネットワークを介してコンピュータに忍び込み、不正動作をしながら他のコンピュータにも侵入していく不正プログラムを指す。ウイルスとの違いは、感染対象（特定のファイルなど）を必要としない点である[11]。
> ・トロイの木馬：通常の有用なアプリケーション（ソフト）の機能を持ち、害のないソフトを装ってはいるが、その陰でシステムやファイルを破壊する悪意あるプログラムである。一般のウイルスのような無意識の感染という形ではなく、自ら招き入れてしまうところからこう呼ばれる[12]。
> ・スパイウェア：ユーザー本人にわからないように個人情報を収集するソフトウェアの総称である。収集された情報は、ユーザーごとに趣味嗜好を加味した広告表示を行うようなソフトウェア（アドウェア）などで利用されることが多いが、利用者が取引しているネット銀行や他のコンピュータのユーザーID、パスワードなどを盗み出すというような使われ方もしている[13]。

このマルウェアの中で最も有名なものに「スタックスネット（Stuxnet）」がある。このウイルスは 2010 年 9 月にイランの核施設で、ウランを精製する遠心分離機を制御するプログラムに到達するまで姿を隠し、ドイツのシーメンス社の制御プログラムに感染すると、モニターには平常であるかのように表示させながら遠心分離機を異常操作し不能にした。多くの重要インフラストラクチャーの制御システムはインターネットには接続されていないクローズド（閉じられた）システムになっているが、この事例でインターネットに接続されていなくてもウイルスに感染する可能性があることが明らかになった。この感染経路は明らかになっていないが、おそらくスタックスネットに感染した USB メモリを誰かが知らずに（あるいは意図的に）施設内へ持ち込んだものと考えられている。このスタックスネットウイルスは従来に比べて非常に洗練されたウイルスであり、これだけの高度なウイルスは個人や民間の組織レベルでの作成は不可能である。アメリカのニューヨーク・タイムズ紙は、イランの核開発を阻止するためにアメリカとイスラエルが共同で仕掛けた一大軍事作戦だったと報じている[14]。

---

[9] コンピュータウイルスに対する予防、発見、駆除、復旧等について実効性の高い対策をとりまとめたもの。経済産業省「コンピュータウイルス対策基準」（http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm）2013 年 11 月 11 日閲覧

[10] 秀和システム第一出版編集部編著（2011）p.74

[11] 大島・堀本（2011）p.1065

[12] 秀和システム第一出版編集部編著（2011）p.513

[13] 大島・堀本（2011）p.714

[14] 伊東（2012）p.78

また、以上のようなマルウェアをばらまいたり、ターゲットに送り込んで対象のシステムに感染させて混乱・麻痺させたりする手法だけでなく、実際に攻撃を開始するはるか前の、ハードウェアの設計開発・製造・流通の段階でその内部のチップにマルウェアを埋め込むことも考えられる。かつてアメリカは「中国製のコンピュータは軍の機微に触れるようなシステムには使用しない」と宣言したことがある[15]。事実アメリカ政府は製品に仕込まれた部品やソフトを利用したスパイ行為・ハッカー攻撃を防ぐ狙いで、2013 年 3 月に成立した暫定予算法に中国製の IT 機器の政府調達を制限する条項を盛り込んでいた[16]。また、イギリス情報機関が世界最大のパソコン企業である中国レノボ社製品の使用を禁止していたことが英紙インディペンデントによって報道された[17]。情報機関がレノボ社製品を調べたところ、外部からの操作でパソコン内のデータにアクセスできる工作が施されているのを発見し、科学者は通常のセキュリティ保護をバイパスする秘密の裏口がチップに最初から仕込まれているとの見解を示したという。オーストラリア政府も 2012 年 3 月、360 億豪ドル（2 兆 9000 億円）に上るブロードバンド事業において、世界第 2 位の中国通信機器メーカー「華為技術（ファーウェイ）」の参入を拒否すると発表した[18]。現地紙によると、その理由は「製品に情報を抜き取る『裏口』が仕組まれているからだ」と報じている。

（3）標的型攻撃

標的型攻撃は APT（Advanced Persistent Threat）攻撃とも呼ばれ、一般に情報摂取等を目的として攻撃対象に潜入し、情報システム内部から有益と思われる情報を摂取するものである。一口に標的型攻撃と言っても、単純に電子メールにマルウェアを添付したものから、巧妙に攻撃シナリオを練ったものまで多種多様である。前者を「ばらまき型」、後者を「やり取り型」という。「ばらまき型」では同じ文面や不正プログラムを多数送信することから、受信者が不審に思う可能性が高まり攻撃の事実が発覚しやすかった。しかし、より巧妙化した「やり取り型」では攻撃者はソーシャル・エンジニアリング[19]を用いる。攻撃者は数か月に渡ってターゲットとなる企業や社員の情報を収集し、社会的な関係（仕事上の関係や会社内の上下関係など）を巧みに利用し、実在する取引相手を装ったり、業務上必要な資料であるかのように偽装し、ウイルスを添付したメールを送りつける。ターゲットの社員は本物のメールと信じて添付されたファイルを開いた瞬間、パソコンがウイルスに感染し、ウイルスはバックドア（裏口）を設けて、遠隔監視のプログラムをパソコンにインストールしてしまう。このプログラムを通して電子メールや機密ファイルへのアクセス、さらにはパソコン周辺環境への録音や撮影が可能となり、多くの場合被害者は自分が被害に遭っていることにすら気づかず、そのまま数年が経っているケースもある。さらに高度な手口では、攻撃者は商品の問い合わせ等を装った通常のメールのやりとりを何通か行うことにより企業の警戒心を和らげる。そして添付ファイル付きのメールが送られても不自然ではない状況を作り出し、その後マルウェアを添付したメールを送りつけて感染させてしまう。

標的型攻撃は 2005 年頃から増え始めた。アメリカ情報セキュリティ大手シマンテックによると、2012 年は世界で 4 万件以上の標的型攻撃があり、2011 年より 42%増えたという[20]。

日本でも、警察庁によると 2012 年における国内の標的型攻撃は 1009 件あった。しかし 2013 年上半期では 201 件と、前年同時期 351 件に比べて 63.6%に留まった。一見攻撃が下火になっているように見えるが、実際は「ばらまき型」が減少し「やりとり型」が増加したのである。「やりとり型」は 2012 年には年間で 2 件であったのに対して、2013 年上半期では半年間で 33 件と大幅に増加した。メールの内容は、5 割超が職員採用に対する質問

[15] 伊東（2012）p.69
[16]「米政府、中国製ＩＴ機器、調達制限――サイバー攻撃に対抗」『日本経済新聞』2013 年 3 月 29 日夕刊
[17]「英情報機関　ハッキング用工作　発見　中国レノボ社製品　PC「使うな」」『東京新聞』2013 年 7 月 31 日
[18]「[サイバーウォーズ 2]（2）知的財産　無防備　情報狙う中国版 OS」『読売新聞』2012 年 7 月 11 日
[19] 巧みな話術や盗み聞き、盗み見などの社会的な手段によって、セキュリティ上重要な情報を入手すること。パスワードを入力するところを後ろから盗み見たり、オフィスの書類ごみをあさってパスワードや個人情報の記されたメモを入手したり、ネットワークの正当な利用者や顧客になりすまして、管理者にパスワードの変更を依頼して新しいパスワードを聞き出す、などの手法がこれにあたる。秀和システム第一出版編集部編著（2011）p.387
[20]「新種のサイバー攻撃――昨年、攻撃世界で 4 万件、拡散防止、対策の主流に」『日本経済新聞』2013 年 6 月 7 日

や応募、約 3 割が製品に関する質問や不具合の報告であった。マルウェアは履歴書、質問状、不具合の状況等を記録した文書ファイルと称して送信されてきた[21]。

３．場

従来、戦場として認識されてきたのは陸上、海上、空中、宇宙の 4 つであった。

しかし2011年7月、アメリカ国防省が「サイバー空間」を陸・海・空・宇宙に続く「新たな戦場の場」として認識し、サイバー攻撃に対して国家をあげて立ち向かうと宣言した。

サイバー空間とはコンピューターやコンピューターネットワーク上の仮想的な空間を意味する。アメリカの「4 年毎の国防計画の見直し（QDR）」では、サイバー空間は「グローバル・コモンズ[22]」であり、それを守らなくてはならないと提言されている。

土屋（2012）によれば、サイバー空間は他の 4 つの戦場とは違って特殊な環境であるという。なぜなら、陸・海・空・宇宙は「自然空間」であるのに対し、サイバー空間は「人工空間」であるからだ。サイバー空間は情報通信端末、情報通信ネットワーク、記憶装置が相互接続されているに過ぎず、それぞれには所有者がいる。それらが全体として確固たるグローバル・コモンズであるかのように見えているが、実は脆弱な基盤に立脚している。また、現代の戦争は通信戦に他ならないため、このサイバー空間が他の 4 つの自然空間すべてに覆いかぶさっていることも重要である。

４．攻撃対象

ネットワークで管理されているすべてのシステムがサイバー攻撃の対象となる。例えば、航空管制システム、交通管制システム、水道制御システム、原子力発電所、金融システム、通信システムなど、枚挙に暇がない。海外では、実際に水道施設の制御システムが外部から乗っ取られた事例もある。オーストラリアの水道運営会社の元契約社員は、雇用を拒否された復讐に下水処理施設の制御システムにハッキングし、約 100 万キロリットルもの汚水を周辺に垂れ流した。元契約社員は制御システム開発に携わっていた技術者だったので、システムの内情に詳しかったのだ。また、スタックスネットの事例も重要インフラストラクチャーを目標にしたサイバー攻撃である。アメリカ国土安全保障省（DHS）によると、2009 年に 9 件だったアメリカでのインフラストラクチャー被害報告は2011年には198件と20倍以上に増加しており、その内水道が 81 件（41%）、電力が 31 件（16%）であるなど、公共性の高いインフラストラクチャーを狙ったサイバー攻撃が半数以上を占めている[23]。日本も経済産業省所管の独立行政法人「情報処理推進機構」（IPA）によると、国の重要インフラストラクチャーを担う企業に標的型メールを送りつけるなどのサイバー攻撃が、2012 年度に少なくとも 246 件あったことが報告された[24]。

５．サイバー攻撃の特徴

以上、サイバー攻撃を構成する 5 つの要素を見てきたが、防衛省（2012）と伊藤（2012）のサイバー攻撃の特徴をまとめると、以下の 5 つを挙げことができる。

第 1 に多様性である。サイバー攻撃に必要な手段は、艦艇や航空機といった従来の兵器と比べて入手・使用が格段に容易であることから、国家だけでなく個人や組織といった様々な主体がサイバー攻撃を実行することができ、インターネットを利用することで世界中のどこからでも実行可能である。

第 2 に匿名性であり、サイバー攻撃は、誰が実行したのかについて、隠蔽・偽装することが容易である。ある国家が他国に対し自ら攻撃を行う、あるいは個人や組織に対象国へのサイバー攻撃を指示、容認することで、自らの関与した形を残さず攻撃の実効性をあげることも考えられる。

第 3 に隠密性が挙げられる。サイバー攻撃の中には、Dos 攻撃のように発生が容易に認識されるものがある一方、マルウェアの埋め込みのように被害が露見するまで防御側が攻撃の存在を察知し難いものや、情報の窃取の

[21] 警察庁（2013）「平成 25 年上半期のサイバー攻撃情勢について」（http://www.npa.go.jp/keibi/biki3/250822kouhou.pdf）2013 年 12 月 9 日閲覧

[22] 一国がコントロールすることはできないが、すべての国が依拠する領域ないし地域を指す。土屋（2012）p.118

[23]「WEDGE Special Report 水も工場も止まる新型サイバー攻撃」Wedge 24 巻 10 号, 2012 年 10 月 pp.36-41

[24]「インフラ企業標的　サイバー攻撃 246 件」『読売新聞』2013 年 4 月 18 日

ようにそもそも被害発生の認識すら困難なものがある。

第 4 に攻撃側の優位性である。攻撃の手法によっては攻撃手段を入手することが容易であること、ソフトウェアの脆弱性を完全に排除することが困難であること、攻撃側は相互連接するネットワークの最も脆弱なポイントをついて攻撃すればよいこと、攻撃元の特定が困難であること等から、サイバー空間においては、攻撃側が防御側に対して圧倒的な優位にある。

そして第 5 に高い費用対効果だ。従来の兵器は、その製造には莫大な費用を必要としたが、サイバー攻撃は優れた知性と創造性をもったハッカーさえいれば、敵に甚大なダメージを与えることができる。

以上のような従来の武力攻撃とは異なった特徴を持つサイバー攻撃に対して、我々はどのような対策を持つべきなのだろうか。次の第 2 章では、現段階での対サイバー攻撃セキュリティの様々な動向を検討していく。

第 2 章　対サイバー攻撃セキュリティ

サイバー攻撃の脅威に対応するため、国際会議や国際連合、国際機関などの場において、サイバー空間に関する行動規範、サイバー攻撃に対する国際法の適用やサイバー空間の在り方に関する議論が活発に行われている。そして国家安全保障や経済成長の観点から「情報セキュリティ」に関する様々な国家戦略が策定されている。ここではサイバー攻撃・サイバー空間に関する法的枠組み、サイバー攻撃に対応する組織を民間・官民・政府別に述べ、軍隊について国際的な取り組みと日本の取り組みを概観し、それらの課題も併せて考察していく。

第 1 節　国際的な取り組み

1．法的枠組み

サイバー空間に対する唯一の国際条約として、欧州評議会が中心となり 2011 年 11 月に採択された「サイバー犯罪条約」がある。これは規制対象を「サイバー犯罪」としており、本論文主旨の「サイバー攻撃」とは異なるものの、サイバー空間における唯一の国際ルールとして重要である。本条約では「コンピュータ・システムに対する違法なアクセス等の行為を犯罪とすること」、「コンピュータ・データの迅速な保全、捜索、押収等の手続きを整備すること」、「サイバー犯罪の犯罪人引渡等の国際協力を推進すること」などを目指されている。2004 年 7 月に発効され、アメリカ、イギリス、ドイツ、フランスなどの欧米主要国をはじめ 37 か国が批准しており、日本でも 2001 年に署名後、国内法整備を進め 2012 年に効力を発揮した。この条約によってサイバー犯罪を非合法化する国際基準はできたが、サイバー犯罪は依然として減少していない。さらに、この条約が規制するサイバー犯罪よりサイバー攻撃は大規模かつ被害が甚大であるため、このような規制だけでは不十分である。サイバー攻撃に対するより包括的な国際ルールの成立が必要になるだろう。

2013 年 3 月にはイギリス・アメリカ・ドイツ・オーストラリアなどの国際法、情報技術、軍事専門家 23 人が NATO サイバー防衛研究所の委託を受け、約 3 年かけて「サイバー戦争」のルールに関する世界初の文書「サイバー戦争に関するタリン・マニュアル」を公表した。タリン・マニュアルでは、国連憲章や傷病者、捕虜の待遇などを定めたジュネーブ条約、国際司法裁判所判例などからなる既存の戦争法は「サイバー空間に適用される」と明記した。タリン・マニュアルでは 95 項目の規則をまとめ、サイバー空間に適用されるとした主な国際法の例を以下に列挙する[25]。

・国家の責任：自国内あるいは政府管理下のサイバー施設が他国への攻撃に使われることを政府は積極的に認めてはならない。

・武力行使・威嚇の禁止：他国の領土一体性や政治的独立を脅かしたり、国連の目的に反するサイバー作戦（cyber operation）は違法である。

・武力行使の定義：サイバー作戦は、規模と効果が通常の武力行使と同じなら、武力行使にあたる。

・対抗措置：損害を被った国は相応の対抗措置を取ることができる。

・自衛権：標的となった国は、個別的・集団的自衛権を行使しうる。

・保護対象：一般市民や医療従事者、医療部隊・輸送手段は保護されねばならず、サイバー攻撃の対象

[25]「サイバー戦争　法整備　英米など専門家指針　国際法を適用　集団的自衛権を行使」『読売新聞』2013 年 4 月 30 日

としてはならない。

世界的なサイバー攻撃の脅威に対処するため、以上のようなサイバー空間における国際ルール作りが推進されているが、いずれも欧米主要国が主導で行っている。このような欧米主要国を中心とした動きに、ロシアと中国は否定的な姿勢を見せており、欧州評議会と対立的な立場にいるのがロシアと中国が加盟している上海協力機構[26]である。ロシアと中国は「サイバー犯罪条約」の締結には反対の立場であり、中国は「我々はこの条約作りに一切関与していない。新しい規範を一から作り直すべきだ」と主張し、欧米主導の枠組みに束縛されることを避けている[27]。

欧米と中国・ロシアは一体何を理由に対立しているのかと言えば、それはサイバー空間における行動規範の方針に関してである。欧米や日本はサイバー空間における「自由な情報の流通」の維持を訴え、対する中国やロシアはサイバー空間の「国家の管理」を強めたがっている。

2011 年 11 月にサイバー空間に関する国際会議がロンドンで開かれた。約 60 か国の政府代表や情報技術企業幹部らが意見交換した。同会議の議長声明において、①世界規模での自由な情報流通、思想・表現の自由を推進・保護し、投資を促進するとともに、国境を越えたサービスの発展を支える政策が求められる旨が確認されたこと、②人権保障を阻害しない範囲でのサイバーセキュリティの確保、言語・文化・思想の多様性の尊重、プライバシー・個人データの保護、デジタル・ディバイドの解消等についての必要性が確認されたこと、などの内容が盛り込まれた[28]。また、会議冒頭でヘーグ英外相はサイバー空間の安定を図るにあたり、基本的人権、特に表現の自由が守られることが重要であり、検閲といった国家による過度な規制は不適切である旨を述べた[29]。

続いて 2012 年 10 月に、ロンドン会議のフォローアップ会議として「サイバー空間に関するブダペスト会議」が開催された。会議には 60 カ国の政府機関他 20 の国際機関、民間セクター、学者、NGO 代表など約 600 名が参加し、サイバー空間における自由と安全保障の両立、開放性や透明性の重要性、サイバー空間における国際行動規範作りの促進、サイバー空間における従来の国際法や国家間関係を規律する伝統的規範の適用などについて活発な議論が行われた。議長声明としてマルトニ・ハンガリー外相は「サイバー空間の恩恵の享受と基本的人権へのコミットメントを失うことなく、これらとサイバー空間におけるリスクの最小化の努力との適切なバランスをとることが重要である。また、サイバー空間の経済的・社会的便益を認識し、人々の安全性とプライバシーを保護する場合を除き、サイバー空間での開放性が確保されつづけるべきである」ことを主張した[30]。

一方、2011 年 9 月にロシア・中国・ウズベキスタン・タジキスタンの 4 か国は国連総会に「情報セキュリティのための国際行動規範」を提出した。この行動規範案では、①テロリズム、分離主義、過激主義を扇動する情報や、他国の政治、経済、社会的安定性や精神的・文化的環境を弱体化させる情報を阻止するために協力すること、②他国の政治経済社会の安全保障に脅威を与えるためにそのリソース、重要インフラ、中核技術やその他の優位性を使用することを防ぐため、ICT[31]製品や ICT サービスの安全を確保するよう努力すること、③情報スペースにおける権利及び自由については、関連する国内法令に従うという前提で十分に尊重すること、などという事項が盛り込まれており、国家によるサイバー空間での主権管轄（国家によるサイバー空間における権利や自由の管理）を強調する内容になっている[32]。

このように、欧米や日本はサイバー空間における「自

---

[26] ロシア、中国、カザフスタン、キルギスタン、タジキスタン、ウズベキスタンの 6 か国からなる地域機構。中国および中国と国境を接する旧ソ連諸国（ロシア、カザフスタン、キルギスタン、タジキスタン）の計 5 か国の首脳が国境地域の信頼醸成および兵力削減について話し合うために開催した年ごとの首脳会議システムである「上海ファイブ」が前進。猪口孝ほか（2005）pp.443-444

[27]「サイバー犯罪捜査　国際ルールの策定難航　欧米と中露対立」読売新聞 2011 年 11 月 5 日

[28] 総務省（2012）p.141

[29] 外務省『サイバー空間に関するロンドン会議について』2013 年 12 月 9 日閲覧（http://www.mofa.go.jp/mofaj/annai/honsho/fuku/yamane/cyber_1111.html）

[30] 外務省『サイバー空間に関するブダペスト会議』2013 年 12 月 9 日閲覧（http://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/cyber_1210.html）

[31] ICT（Information and Communication Technology）とは、従来の IT（Information Technology）の概念を一歩進め、情報にコミュニケーションの重要性を加味した概念を含む情報通信技術を表す言葉である。国際的には IT よりも普及している。大島・堀本（2011）p.177

[32] 総務省（2013）pp.140-142

由な情報の流通」の維持を訴え[33]、対する中国やロシアはサイバー空間上の情報統制を重要視すべきであるという立場を主張している。このため、国際社会において一貫したサイバー空間の国際ルール作りには困難を極めるだろう。

２．セキュリティ組織

サイバー攻撃に対応するための組織も政府、官民、民間といった形で設置される。ここでは国際的な動向や組織を扱い、特にアメリカは組織構築が他国に比べて進んでいるため、アメリカの組織を主要なものとして紹介する。

インターネットを介して発生するコンピュータ・セキュリティ・インシデントに対応する活動を行う組織を「CSIRT（Computer Security Incident Response Team）」と呼ぶ。企業内部に属して自組織対応するCSIRT、国や地域の情報をまとめ他の CSIRT と情報交換を行う CSIRT、特定の顧客に有償のサービスとして復旧までを行うセキュリティベンダなどがある[34]。

その起源は CERT/CC（Computer Emergency Response Team/Coordination Center）と言われている。CERT/CC はクラッキングやウイルスの蔓延、その他コンピュータセキュリティにかかわる事象に対応するために設けられた非営利組織であり、アメリカカーネギーメロン大学内に事務局を置く[35]。CERT/CC を含めた CSIRT は、事態収拾のために率先して告発や摘発を行うわけではなく、情報の収集と対応策の分析や広報、利害組織間の仲介を基本任務としている。

また、官民組織として NCFTA（National Cyber-Forensics and Training Alliance）がある。これはアメリカ連邦捜査局（FBI）や情報セキュリティ会社大手のシマンテック（Symantec）、情報技術に強いカーネギーメロン大学など産官学のメンバーで構成する団体で、1997 年に設置された。官民がサイバー犯罪の手口やウイルス情報をデーターベースに蓄積し、主に大学の研究者が研究し、捜査員が対応できるよう訓練する組織である[36]。

NATO ではサイバー防衛に関する研究機関である NATO サイバー防衛センター（CCD COE; Cooperative Cyber Defence Centre of Excellence）が 2008 年に設置された[37]。

３．軍隊

サイバー攻撃に対処するための部隊の整備が世界で着々と進められている。しかしその内容は軍事機密になるため中々サイバー軍の実態を探ることは難しい。ここでは世界各国がサイバー攻撃に対してどのような軍備整備を進めているのか、断片的ではあるが紹介する。

国連軍縮研究所によると、2013 年 4 月の時点で世界の約 4 分の 1 に当たる 46 か国がサイバー戦をにらみ、専門部隊を創設したり有事作戦立案を進めるなど軍事・防衛分野の取り組みを進めているという。2011 年の調査では 33 か国だったが新たに日本を含め 13 か国が増え、各国がサイバー攻撃への対策の推進を加速させている現状が浮き彫りになった[38]。

サイバー先進国とも言われているアメリカでは、2010 年にサイバー空間における作戦を統括する部隊「サイバーコマンド」を創設した。今後、この部隊を①敵へのサイバー攻撃を行う「戦闘任務部隊」、②国の基盤施設を守る「国家任務部隊」、③アメリカ軍のコンピュータ・システムを守る「サイバー防衛部隊」の 3 部隊を新設する予定である。また、今後 4 年間で要員を 4 千人増やすとともに、ネットワーク強化などサイバー安全保障対策に 230 億ドル（約 2 兆 3 千億円）を投入する[39]。

イギリスでは、国防省は 5 億ポンド（約 800 億円）の予算を組んで、サイバー空間の防衛と攻撃に備える「統合サイバー予備軍」を立ち上げるとフィリップ・ハモンド国防長官が述べた。「統合サイバー予備軍」では数百人規模のハッカー達を入隊させる予定であり、既存の統合

[33] もっとも、2013 年 6 月に発覚した元 CIA のスノーデン氏が暴露した米国家安全保障局（NSA）による大規模な情報監視活動や、日本の特定秘密保護法案成立を考えれば、けっして欧米や日本も「自由な情報の流通」を実質目指しているとは言い難いだろう。
[34] 相戸（2007）p.183
[35] 秀和システム第一出版編集部編著（2011）p.881
[36]「警視庁、サイバー犯罪対策新組織、産官学が連携、創設へ有識者懇」『日本経済新聞』2013 年 7 月 4 日夕刊
[37] 防衛省（2013）p.83
[38]「サイバー戦 46 カ国対策　専門部隊創設など、日本も着手」『静岡新聞』2013 年 4 月 28 日
[39]「広がるサイバー攻撃（4）変容する防衛・同盟――理論的整理が課題（時事解析）」『日本経済新聞』2013 年 7 月 18 日；「米軍、サイバー防衛強化、司令部要員 4 年で 4000 人増」『日本経済新聞』2013 年 6 月 28 日夕刊

サイバー部門を支援する形になる。統合サイバー予備軍の徴募の対象は、イギリス国防軍を除隊する正規兵、必要な技能を持つ現役予備兵および元予備兵、そして過去に軍隊の経験はないが必要なIT技術を身につけている個人の3つのグループである[40]。

韓国では2010年1月に、サイバー空間における作戦の計画、実施、訓練および研究開発を行うサイバー司令部が設置され、国防部直轄部隊として運営されている。今後は兵力を2倍の約1000人に増やす計画である。

中国のサイバー部隊に関して、アメリカ情報セキュリティ会社マディアントは2004年以来の数百の企業・組織へのサイバー攻撃を追跡調査した結果、上海に拠点を置く中国人民解放軍総参謀部所属の「61398 部隊」がサイバー攻撃を行っていると結論づけた[41]。また台湾当局の分析では、総参謀部が率いるサイバー部隊は約40万人いるとされている。上海の部隊は指揮・指令の核であり、配下の学校や教員や学生らが実働部隊を担っているとみられている[42]。

北朝鮮では金正日総書記の時代からサイバー戦力を強化しているという。1986年にはコンピュータ教育に特化した「美林大学」を設立し、現在は年間60人ほどのハッカーを養成しているとされる。韓国政府は北朝鮮のサイバー戦力について、数千人規模の人員がいるとみている[43]。加えて韓国の情報機関・国家情報院は金正恩政権がサイバー戦力を強化し、総員約1700人のハッカー専門部隊を設置したと明らかにした[44]。また、同院は表向きソフトウェア開発である北朝鮮国営企業「朝鮮コンピューターセンター（KCC）」関係者の約4200人も、サイバー戦の支援戦力とみている。

第2節　日本の取り組み

ここでは日本の取り組みを法的枠組み、セキュリティ組織、軍隊としての自衛隊の3つを概観していく。国際的なサイバー防衛の動向に対して、比較的対応が遅いと言われている日本では、積極的にサイバー攻撃に対処しようという傾向が強まってきたのはここ2、3年の間であり、従ってサイバー先進国と言われるアメリカなどに比べるとその動きは組織間の足並みがとれていないように思われる。以下、3 つの分野において日本の取り組みと現状、それらの課題について考察していく。

1．法的枠組み

現在、日本においてサイバー犯罪に対応する警察法規には以下の3つのタイプが挙げられる。

第1にコンピュータ・電磁的記録対象犯罪であり、刑法に規定されているコンピュータや電磁的記録を対象とした犯罪である。コンピュータを操作して他人を騙し、不正に財産を得ることを禁止した「電子計算機使用詐欺罪」（刑法246条の2）、またはコンピュータやデータを破壊して業務を妨害することを禁じた「電子計算機損壊等業務妨害罪」（刑法234条の2）、他人の事務処理を誤らせる目的で電磁的記録を不正に作ったり供したりすることを禁じた「電磁的記録不正作出及び供用罪」（刑法第161条の2）などがある。具体的な犯罪の例を挙げると、金融機関のオンライン端末を不正操作し無断で他人の口座から自分の口座に預金を移したり、サーバコンピュータに保存されているホームページのデータを無断で書き換えたりした場合、このタイプの刑法違反となる。

第2に、ネットワーク利用犯罪である。上記のコンピュータ・電磁的記録対象犯罪以外で犯罪の実行にネットワークを利用した犯罪、または犯罪行為そのものではないものの、犯罪の敢行に必要不可欠な手段としてネットワークを利用した犯罪である。具体的に、刑法においては「詐欺罪」（刑法246条）、「名誉棄損罪」（刑法230条）、「わいせつ物頒布等の罪」（刑法175条）に違反する行為がネットを利用して行われる犯罪である。その他「出会い系サイト規制法」、「児童買春・児童ポルノ禁止法」、「著作権法」、「商標法」、「売春防止法」などもあてはまる。たとえば、インターネットオークションで自分が持っていない品物を出品して落札者から代金を騙し取ったり、インターネット上にわいせつな映像や画像を掲載するなど、犯罪の実行にあたりネットワークを利用した場合が

---

[40]「英国防省、「数百人のハッカー」を募集」産経ニュース2013年10月1日
（http://sankei.jp.msn.com/wired/news/131001/wir13100118140000-n1.htm）2013年12月16日閲覧

[41]「「サイバー攻撃元は中国部隊　米標的 国家ぐるみ　米情報会社が報告書」『読売新聞』2013年2月21日

[42]「サイバー部隊中国で膨張、軍傘下の大学、精鋭生む」『日本経済新聞』2013年3月5日

[43]「北、サイバー戦力強化　対韓攻撃の疑い　中国、拠点黙認か」『読売新聞』2013年3月22日

[44]「北、1700人ハッカー部隊　正恩氏「サイバー戦力は宝剣」」『読売新聞』2013年11月6日

これにあたる。

第3には「不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）」である。2000年2月13日に施行され、刑法で定めたような直接の被害が発生しなくても、権限を持たないものが勝手にアクセスする行為及びそれを助長する以下の行為を罰することができるようになった[45]。

・他人のパスワードを利用し、正当な利用者に「なりすまし」て侵入（第3条の1）

・パスワード認証を迂回するセキュリティホールなどを利用して侵入（第3条の2）

・踏み台となるコンピュータを経由して侵入（第3条の3）

・他人のパスワードを許可なく第三者に教える（第4条）

第5条では、システム管理者は担当する当該システムが不正アクセスに遭わないように、常に適切な管理措置を講じる必要があると規定されているが、これは努力義務にとどまり違反しても罰則等の制裁は課されないため、この第5条においてはその実効性が疑問視されている。

さらに、以上3つのタイプの警察法規に新しく「不正指令電磁的記録作成罪（ウイルス作成罪）」が2011年6月に加わった。ウイルスを「意図に反する動作をさせるべき不正な指令を与える電磁的記録」と定義し、コンピュータ・ウイルスなどを「作成すること（作成）」「提供すること（提供）」「誰かに送りつけたり、知らないうちにダウンロードさせること（供用）」「ウイルスと知りながら手に入れること（取得）」「保管すること（保管）」を禁止した[46]。この成立の背景には、これまで日本にはウイルス作成を罪に問う法律がなく、警察は器物損壊罪や著作権法違反などを「駆使」して摘発せざるを得なかったという事情があった[47]。また、これは「サイバー犯罪条約」が求める国内法整備の一環で創設されたものである。これまで摘発に苦慮してきた捜査当局は成立を歓迎するが、プログラムの欠陥はウイルス同様に意図に反する動きを生じさせる場合もあるため、ネット業界からは「法律の趣旨が拡大解釈され、濫用されないか不安」と懸念する声もあがっている[48]。

２．セキュリティ組織

日本の情報セキュリティに対応する代表的な組織に「JPCERT コーディネーションセンター（JPCERT/CC[49]）」がある。日本の代表的なCSIRTであり、政府機関、企業から中立な団体として1996年に発足した。侵入やサービス妨害などのコンピュータセキュリティ・インシデントについて、報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討と助言などを技術的な立場から行っている[50]。

また、日本政府の各省庁も様々な活動や組織を立ち上げており、省庁別にそれらの概要を見ていく。

まず日本の情報セキュリティ戦略において中心的な役割を担うのが「内閣官房情報セキュリティセンター（NISC[51]）」である。2005年に内閣官房に設置され、日本の情報セキュリティ政策の立案、国際的な連携、情報分析、政府機関への支援、官民連携によるインフラ対策などを進めている。だが、NISCのスタッフは各省庁からの出向者が多く、権限もほとんど持たないため深刻化するサイバー攻撃に十分対応できないことが課題になっている。NISCは司令塔機能を強めるため、2015年度をめどに専門職員を増やすなどNISCの態勢を強化して「サイバーセキュリティセンター（仮称）」への改組を目指している[52]。

経済産業省は若手ハッカーによるサイバー攻撃対応チームを組織し、被害企業に派遣する方針を打ち出した。経産省の補助金を受け、独立行政法人である情報処理推進機構（IPA）が来年度から毎年、十数人の若手技術者を雇用し、養成課程で解析技術やマネジメント、コミュニケーション技術などの研修を実施したうえで、経験豊富な技術者をリーダーとするチームに組み入れ、被害を届

45 相戸（2007）p.251
46 伊東（2012）pp.206-207
47「ウイルス作成罪　捜査当局から歓迎の声　ネット業界『乱用に不安』」『読売新聞』2011年6月17日
48「ウイルス作成罪成立へ　今国会で　サイバー犯罪摘発へ期待」『読売新聞』2011年6月6日
49 Japan Computer Emergency Response Team/Coordination Center
50 相戸（2007）p.185
51 National Information Security Center
52「サイバー攻撃対策、実効性は　情報セキュリティー、政府が新戦略」『朝日新聞』2013年08年01月

け出た企業に派遣する[53]。

総務省では中央省庁のシステム担当者らを集め、実践的なサイバー防御演習を開始し、2014 年度は大企業などにも対象を広げる予定である[54]。

また、情報セキュリティ対策は組織間の情報共有が重要である。サイバー攻撃の手口はますます巧妙化・複雑化し、単独の組織では対応が難しくなっている。そのため、サイバー攻撃に適切に対処するため、最新のサイバー攻撃の手口や傾向、様々な脆弱性情報、関連する攻撃予兆情報、攻撃対象となった企業分野などの情報を共有することにより、迅速に対応できるような情報共有の場が必要である。国内では、これまで官主導で組織づくりが進められてきたが、ここにきて民間主導の情報共有も進んでいる。日本の主なサイバー攻撃情報共有の取り組みを官主導と民主導に分けて表 2 にまとめた。

官主導では、経済産業省はサイバー攻撃の被害防止のため、官民でサイバー攻撃の情報を共有する組織「サイバー情報共有イニシアティブ（J-CSIP[55]）」を発足させた。攻撃の特徴や手口を共有し各社の防御態勢強化につなげ、全5業界と45の参加組織による情報共有体制を確立している。テレコムアイザック官民協議会では、サイバー攻撃に関する情報共有や対応策の強化に向けた議論をするとともに、所管の電気通信および放送分野の事業者や地方公共団体等との連携の充実に努めている[56]。「サイバーディフェンス連携協議会」は、サイバー攻撃に対し防衛省と防衛産業の間で協力を図り、企業に送られてきたウイルスの性質などについて情報共有する。将来的には防衛省と防衛産業がサイバー攻撃対処のための共同訓練を視野入れている[57]。

民主導の「サイバーリスク情報センター」では、攻撃手法や企業側の被害の状況を分析し、攻撃された企業名などを伏せたうえで、攻撃の狙いをわかりやすく解説したり対処法を助言したりする[58]。「サイバー・グリッド研究所」では、ハッキングやウィルス解析、スマートフォンのセキュリティ確保など 7 分野を研究し、共有する情報を増やし、未知の攻撃に遭った企業に対して、復旧から再発防止策の浸透までを 2 週間程度で提供できるようにする[59]。

しかし、日本企業は欧州に比べて情報提供の意識は低いという指摘もある[60]。加えて、サイバー情報共有イニシアティブでは企業が情報を政府機関に提供しても見返りが少なく、会社の評判が悪くなるのを懸念して攻撃を受けた事実を公表したがらない傾向もあり、企業側の消極的な姿勢が課題であるという指摘もある[61]。当然他の情報共有組織について同様であり、組織が情報セキュリティに対して有効な対策を構築するにはまだ時間がかかると思われる。

警察では、まず全国的に 13 都道府県の警察本部に「サイバー攻撃特別捜査隊」を創設し、サイバー攻撃の捜査に専従させ、全国で 140 人態勢で情報収集や被害防止に当たっている[62]。また警察庁では「サイバー攻撃分析センター」を約 20 人で新設し、全国の警察の司令塔としてサイバー攻撃に関する情報の収集や分析、捜査の指導調整などに当たる[63]。警視庁ではサイバー犯罪対策課の捜査員を 2014 年中に約 60 人増員し、サイバー犯罪の初動捜査を支援する「機動サイバー班」、インターネットバンキングの不正送金事件を担当する「生活安全部長匿名捜査班」、不正アクセスや新型ウイルスの研究にあたる専門チームなどの専従班を発足する[64]。

だが政府機関、特に警察において様々な組織がばらばらに新設されており、サイバー攻撃・犯罪に対して一元的に対処できないという課題が挙げられる。

3．自衛隊

現在自衛隊には陸海空自衛隊から独立している「指揮

53「『正義のハッカー隊』発足へ　サイバー攻撃　被害企業に派遣　経産省」『東京読売新聞』2013 年 8 月 30 日夕刊
54「省庁でサイバー防御演習へ」『朝日新聞』2013 年 09 月 20 日夕刊
55 Initiative for Cyber Security Information sharing Partnership of Japan
56 総務省（2012）p.151
57「対サイバー攻撃協議会発足」『朝日新聞』2013 年 7 月 13 日
58「NEC・NTT など、サイバー防衛で連携、海外情報も収集」『日本経済新聞』2013 年 11 月 28 日
59「情報セキュリティー各社、サイバー攻撃対策で連携」『日本経済新聞』2013 年 11 月 25 日
60「サイバー攻撃、連携で阻止、世界、ICPO が対抗拠点、国内、企業主導で情報共有」『日経産業新聞』2013 年 11 月 29 日
61「『正義のハッカー隊』発足へ　サイバー攻撃　被害企業に派遣　経産省」『読売新聞』2013 年 8 月 30 日夕刊
62「サイバー攻撃、専従部隊発足」『日本経済新聞』2013 年 04 月 02 日夕刊
63「サイバー対策司令塔新設　技術部隊、全国に一警察庁」『静岡新聞』2013 年 5 月 16 日夕刊
64「サイバー犯罪捜査に新組織、警視庁、初動支援や新型研究」『日本経済新聞』2013 年 09 月 20 日夕刊

通信システム隊」、陸上自衛隊の「システム防護隊」、海上自衛隊の「保全監査隊」、航空自衛隊の「システム監査隊」の 4 つの部隊があり、約 360 人態勢で防護を担当している。これまでサイバー空間の脅威情報の収集や研究はバラバラに行ってきたため、自衛隊はサイバー攻撃に対して一元的に対処することができなかった。そこで防衛省は激化するサイバー攻撃への積極的に対処するため、2013 年度末に指揮通信システム隊の下部組織として 100 人規模の「サイバー防衛隊」を発足させることを発表した。高度な知見を持った専門家部隊と位置付けられ、任務は①全部隊の運用を一元管理する「中央指揮システム」の 24 時間監視、②ウイルスなど脅威情報の収集と共有、③サイバー戦を想定した模擬演習、④新たな攻撃手法に関する研究、⑤陸海空への技術支援の 5 項目である。

また、防衛省が対サイバー兵器を開発していることも報道された[65]。これはサイバー攻撃を受けた際にその攻撃元を探り当てる逆探知機能があり、直前の攻撃元だけでなくそのコンピュータを「踏み台」として操っているコンピュータまで次々と探索していくことができる。また、攻撃元を無力化したり、情報収集を行ったりする機能も持ち合わせている。2008 年から開発に着手し、現在は閉鎖されたネットワーク環境下で運用しながら、試験的に運用している。関係者によると DDoS 攻撃や標的型攻撃の攻撃元をかなりの確率で辿ることが可能であるという。

しかし、日本では有事法制でサイバー攻撃を想定しておらず、対外的な運用には新たな法解釈が必要となる。自衛権が発動できる「武力攻撃事態」の 4 類型にサイバー攻撃は含まれておらず、現状では使用すれば刑法のウイルス作成罪などに抵触する可能性もある。

第 3 章　考察

これまで第 1 章ではサイバー攻撃の特徴、そして第 2 章で対サイバーセキュリティ対策における国際的・日本国内の取り組みを見てきた。第 3 章ではサイバー攻撃に対する自衛権と先制攻撃、予防攻撃についてその是非と、日本の情報セキュリティ政策を考察したい。

1．自衛権と先制攻撃・予防攻撃

サイバー攻撃は国家の安全保障に対する脅威と認識されている。サイバー攻撃に対して各国はサイバー空間に特化した軍隊や、法的措置、情報セキュリティの構築など、様々な措置をとっている。

しかしサイバー攻撃は従来の武力攻撃とは違い、運動エネルギーを伴わない特徴がある。国際法と国際社会がこれまで認識してきた武力攻撃と概念が違うサイバー攻撃に対して、国際法はどのように対応すればよいのだろうか。そして、重大な損害を与えて国家の安全を脅かすサイバー攻撃に対して、軍事力を用いて反撃することは国際法的に許されるのだろうか。これらの論点はこれまでの章の中で言及されている部分もあったが、ここで改めて議論を整理し、検討する。最初にサイバー攻撃に対して国際法的な視点で述べ、次に日本の法的見解を取り扱う。

サイバー攻撃を武力攻撃と解釈できるか否かを検討する前に、まず国際法上の自衛権の概念について考察する。

自衛権の行使にあたって、その発動が「武力攻撃の発生」の場合に限られるか否かを巡って激しい学説上の対立がある。その争点は「武力攻撃」に限られるか否かという問題と、その「発生」の場合に限られるか否か（つまり「先制的自衛権」は許容されるか）という 2 点に分けられる。前者は、自衛権行使は国家の領域的一体性と政治的独立を侵すような現実に発生した武力攻撃に対してのみ許されるとする「制限的解釈説」と、自衛権行使は直接の武力攻撃以外（たとえば間接侵略）も対象とし、また国家の本質的利益（たとえば在外自国民の生命・財産や国家の存外権益）も保護法益として認める「許容的解釈説」との間で対立してきた[66]。従来は「制限的解釈説」が通説的地位を占めていたが、それではサイバー攻撃は現実に発生した武力攻撃ではないため「武力攻撃」と認識されないのだろうか。

結論から言えば、一部の重大なサイバー攻撃は武力攻撃として認識されつつある。最初の Hathaway らによるサイバー関連用語の定義も、サイバー攻撃が現実の武力攻撃と同等であるなら「サイバー戦争」となると定義し

[65]「防衛省が対サイバー兵器　逆探知し無力化　政府、法対応に着手」『読売新聞』2012 年 1 月 1 日

[66] 小寺ほか（2004）p.450

ていた。タリン・マニュアルの規則 11 でも「サイバー作戦は、その規模及び効果が武力の行使の水準に至る非サイバー作戦に比肩しうる場合には、武力の行使に該当する」と規定している。では何が武力攻撃に相当するかについては、タリン・マニュアルでは「規模と効果」を判断基準とした。その判断基準となりうる８つの要因は①結果の重大・深刻性、②即時性、③直接性、④侵入性、⑤結果の計測可能性、⑥軍事的性質の有無、⑦国家の関与の程度、⑧合法性の推定[67]、などである[68]。

サイバー攻撃が武力攻撃とされれば、当然それに対する自衛権の発動の問題につながる。国連憲章第 2 条 4 項は武力行使を禁止しているが、その例外として国連憲章第 51 条は他国による武力攻撃が発生した場合、安全保障理事会が必要な措置を取るまでの間、国家は自衛権を発動して武力行使することを「固有の権利」として規定している。同条は、外国からの違法な侵害に対して反撃のために必要な限度で武力を行使する権利を「個別的自衛権」と呼び、また同様の場合に、加盟国が集団で反撃できる権利を「集団的自衛権」と規定した[69]。個別的自衛権は単独で危害を排除する権利であるのに対して、集団的自衛権は他国への脅威を自国への脅威と見なして反撃する権利である[70]。サイバー攻撃に対して個別的・集団的自衛権の発動が可能かという問題では、タリン・マニュアルの規則 13 では「武力攻撃の水準に至るサイバー作戦の標的である国家は、固有の自衛権を行使することができる」としている。

サイバー攻撃の効果が武力攻撃に相当すれば、攻撃された国家は自衛権を発動できることがわかった。ではサイバー攻撃を受けた国家は、自衛権及び対抗措置としてサイバー攻撃によって反撃できるのだろうか。中谷（2013, p.61）によれば、アメリカ国務省法律顧問 Harold Koh は「サイバー武力攻撃に対する反応は必要性及び均衡性の要件を満たす限りサイバー行動の形態をとらなければならないとの法的要件はない」としており、つまりサイバー攻撃に対する反撃でサイバー手段を使用するには当然許容されると解釈してもよいだろう。タリン・マニュアルもサイバー攻撃による反撃は当然可能との前提に立っている。

続いて自衛権行使の際の 2 つ目の争点である先制的自衛権に関してだが、自衛権行使の中に 2 つの概念が存在している。それは「先制的自衛権」と、「予防攻撃」ないし「予防戦争」である。ナイ（2011, p.250）によれば、「予防的先制戦争と予防戦争の間には違いがある。予防的先制攻撃は戦争が今にも起りそうなときに発生するのに対し、予防戦争は、今仕掛けた方が後で仕掛けるよりもよいと指導者が判断した時に発生する戦争なのである。」ナイの言う前者の先制的自衛権の概念を認めるか否かに関する議論はあるが、武力攻撃が真に急迫している場合は国家が自衛権を行使しうるとする点で共通理解されており、後者は違法とされている[71]。

では、サイバー攻撃に対してサイバー手段による反撃が許されるのであれば、外国から攻撃されそうな場合はサイバー攻撃によって先制攻撃および予防攻撃を行うことはできるのだろうか。

タリン・マニュアルを作成した専門家の一般的見解は、先行自衛[72]は認めるが予防自衛[73]は認めないというものである[74]。また、オバマ政権は外国からサイバー攻撃が行われるとの確証を得た場合、大統領が先制攻撃を命令できるとする政策をまとめた[75]。しかし、第 1 章のサイバー攻撃の特徴でも述べた通りサイバー攻撃は攻撃元を詐称することは容易であり、複数国を経由するなど攻撃主体の特定が非常に難しい。

さらにブッシュ政権は、9.11 事件およびその後のイラク戦争において「先制」という言葉を予防戦争の色彩を帯びた概念として用いたため、概念的に異なる「先制」と「予防」、および「差し迫った脅威」と「潜在的脅威」の区別を曖昧なものにしてしまった[76]。従ってサイバー攻撃による先制攻撃と予防攻撃の判別はより困難であり有

[67] 明確な条約または一般に認められる慣習法の禁止がなければ、行為は合法的であると推定される。例えば国際法はプロパガンダや心理戦、スパイ活動、単なる経済的圧力それ自体を禁止していないため、これらのようなカテゴリーに分類される行為は合法的であると推定される。このように、それらの行為は国家によって武力行使とみなされる見込みはほとんどないだろう。CCD COE（2013）p.51, 2013 年 12 月 23 日閲覧
[68] CCD COE（2013）p.48, 2013 年 12 月 23 日閲覧
[69] 加藤・渡邊編（2002）p.159
[70] 加藤・渡邊編（2002）p.30
[71] 小寺ほか（2004）p.450
[72] 先行自衛はナイの言う予防的先制戦争にあたる。
[73] 予防自衛はナイの言う予防戦争にあたる。
[74] 中谷（2013）p.60
[75]「米、サイバー戦で先制攻撃も」『日本経済新聞』2013 年 2 月 5 日夕刊
[76] 岡垣（2006）p.17

効的ではないかもしれないが、許される攻撃と許されない攻撃の区別は重要である。

一方日本においては憲法 9 条との兼ね合いが重要になってくる。自衛隊の自衛権発動の 3 要件は①我が国に対する急迫かつ不正の侵害があること、②これを排除するためにほかの適当な手段がないこと、③必要最小限度の実力行使にとどまるべきこと、である[77]。また、政府は現在、武力攻撃事態について①着上陸侵攻、②ゲリラ・特殊部隊による攻撃、③弾道ミサイル攻撃、④航空機による攻撃の 4 類型を想定しており、ここにはまだサイバー攻撃は加えられていない[78]。

防衛省はサイバー攻撃に関する指針の中で、弾道ミサイルや航空機による攻撃と共にサイバー攻撃が行われた場合は、これを「急迫不正の侵害」と認定し、自衛権を発動する要件の一つを満たすと明記した[79]。しかし、通常兵器による攻撃を伴わずサイバー攻撃が単独でされた場合に関しては「引き続き検討する」と述べており、いまだ不明瞭のままである。安倍首相も「サイバー攻撃と自衛権行使の関係は個別具体的な状況を踏まえて判断すべきもので、一概に述べることは困難だ」と語っている[80]。

サイバー攻撃に対する自衛権の認識は、日本は慎重な態度を取っているのに対し国際社会は一歩先に進んでいるように見える。日本政府は往々にして様々な政策が海外に比べて遅れていると批判されているが、ここでも対策の構築が遅れているという非難が多くの研究者から指摘されている。だが、私はサイバー攻撃を武力攻撃と同等と考えるのは時期尚早であると考える。サイバー攻撃を武力攻撃と同視し、自衛権の行使を認め反撃も可能という考えが国際社会の中に行きわたることに疑問を禁じ得ない。サイバー攻撃は攻撃元がわかりにくく、その攻撃元を割り出す技術も未熟なままでサイバー攻撃に対する自衛を積極的に認めれば、それは諸外国との間に軋轢を生むことになるだろう。バレリアーノ (2013, pp.92-94) らの研究によれば、分析対象とした 95 のサイバー攻撃のうち、「スタックスネット」のような脅威度の高い攻撃はわずか 3 件しかなかった。現実世界における様々な脅威や攻撃に比べてサイバー攻撃の数は非常に少なく、国家はサイバー攻撃に遭うリスクよりもテロに遭うリスクの方が 600 倍も高い。パネッタ国防長官は「サイバーセキュリティ予算を最優先にする」と表明し、アメリカ国防省は 2012 会計年度にサイバーセキュリティのために 26～32 億ドルを投入している。アメリカ空軍だけでも、2013 年に 46 億ドルをサイバーセキュリティに投資することを計画しているが、バレリアーノらは「国家がサイバー戦争に対する防衛体制を整備するのは当然のことだが、莫大な資金を低レベルの脅威対策のために投入するのは馬鹿げている」と述べている。以上のようなことを考えると、サイバー攻撃に対する自衛権は、重大な物理的な損害を持つ攻撃に限定されなければならず、安易に認めるべきではない。Dinniss（2012, p.113）も「コンピュータ・ネットワーク攻撃に関して、武力攻撃の基準点とそれに伴う自衛権に関する限定的な見解が望ましいと考える。従って、武力攻撃に達するコンピュータ・ネットワーク攻撃の分類は、資産または人への物理的攻撃を引き起こす攻撃に制限されなければならない」としている。

加えて軍のサイバー部門関連に多額の予算が付くことにも警鐘を鳴らしたい。軍産複合体という用語があるが、これは兵器生産を担当する軍需産業界と、軍事力強化を目指す軍部とが形成する利益共同体を指す。対外的な脅威を強調することにより国防支出の増額を目指す軍事的エリートが、国家安全保障政策の形成に重要な役割を果たすという議論もこの延長線上のものである [81]。アメリカのアイゼンハワー大統領が離任演説で用いた言葉で、軍産複合体の肥大化によってアメリカの自由と民主主義という基本理念が損なわれると警鐘を鳴らしたことにより、広く知られるようになった。谷口（2012）はその軍産複合体が兵器産業だけに留まらずサイバー空間をも飲み込み、新しい脅威と伴って生成されているサイバー軍産複合体の膨張を警告している。軍の高官や軍需産業の幹部らが自身の分野に多額の政府の予算をつけさせるために、実体のないサイバー攻撃の脅威を大々的に宣伝していることも考えられる。

---

77 中谷（2013）p.61

78「サイバー攻撃「新たな戦争」　自衛権発動　武力攻撃認定が課題」『読売新聞』2012 年 1 月 1 日

79「サイバー防衛「新たな戦場」国全体で対応を」『読売新聞』2012 年 9 月 7 日夕刊

80「サイバー防衛、体制強化急ぐ、首相「自衛権発動の対象」、米との連携協議も」『日本経済新聞』2013 年 10 月 24 日

81 岩内、藪野編（2003）p.44

以上の研究や考察を踏まえると、サイバー攻撃という言葉がメディアや軍事関係者によって誇張されているように感じる。サイバー攻撃の現状より先走って議論を進めてしまい、安易に武力攻撃と認定してしまえば各国との間で軋轢を生むことになる。サイバー攻撃への対応がエスカレートすれば、それは戦争に発展する危険性が高まることを意味する。サイバー攻撃は確かに脅威だが、しかし高度なサイバー攻撃、または武力紛争の中で行使されるサイバー攻撃は十分な資金と専門家集団が必要になる。そのような専門家集団が遂行し、武力攻撃にも達しうるサイバー攻撃と、国家への影響が軽微なサイバー犯罪の区別は重要である。サイバー攻撃に対する情報セキュリティは重要であるが、しかしそれらの議論が現状より前のめりになってしまってはいけない。誇張されているサイバー攻撃という言葉の中から、本当に脅威的な攻撃と軽微な犯罪を見分けることが求められているだろう。

2．日本のセキュリティ政策への提案

（1）情報セキュリティに関する「抜き打ち検査」の実施

今日のサイバー攻撃への法的束縛に関する議論が未熟である上に攻撃元が明確でない性質を持っているため、サイバー攻撃への対応は攻撃されにくいようにセキュリティを向上させることが最も有効な対処策になる。だが、そのすべてを政府が担うことは実質難しいだろう。政府はセキュリティ向上の支援や情報共有組織の設立、情報セキュリティ方針を立てるというようなサポートが限界だ。つまり実際のセキュリティ向上はその組織が主体となって行うべきであり、民間レベルが現実的である。

政府と民間のネットワークは相互作用しており、政府へのサイバー攻撃も個人のコンピュータを踏み台にする場合もあるため、サイバー攻撃を仕掛ける側にとって、民間ネットワークやコンピュータは非常に魅力的な目標となりうる。つまり国家の安全保障の観点からも民間と経済面でのセキュリティ向上は非常に重要である。

第 2 章の日本の取り組みで述べたように、様々な企業やインフラストラクチャーが利用しているシステムのセキュリティを高めようと、情報共有組織やサイバー攻撃に対する模擬演習などが実施されている。

サイバー攻撃に対するセキュリティは、もはや対策ソフトだけでは限界がある。今日のサイバー攻撃はソフトの脆弱性、システムの設定不備、人間の心理、組織情報を巧みに利用した攻撃である。セキュリティ構築にはサイバー攻撃を念頭に置いた組織作りや意識喚起など、人間的なセキュリティの向上が必要になっている。

しかしその人間的なセキュリティの向上を図ったところで、実際構築したセキュリティが本当に効果的であるのかを確認することは難しい。そこでセキュリティ向上を図る中で、民間の IT 企業はサイバー攻撃から企業を守るセキュリティ診断サービスを提供している。たとえば伊藤忠テクノソリューションズは、企業が攻撃にどの程度耐えられるかをシステムと組織の両面から総合診断し、対策を包括提案するサービスを始めた[82]。野村総合研究所グループは疑似の標的型メールで攻撃し社員を訓練するサービスを提供している。他にも日本の IT 企業のラックや日立ソリューションズ、アメリカ大手企業シマンテックなど各セキュリティ会社もセキュリティ診断サービスを提供している。

また、サイバー攻撃に対する安全性を定める安全基準をまとめる取り組みが日米間で始まっている。海外ではメーカーの製品に対して、サイバー攻撃をはね返したり被害を最小限にとどめたりする安全基準を国際規格にしようとしているアメリカ研究機関「ISCI（ISA Security Compliance Institute）」がある。日本国内のメーカーが電力の制御装置などを海外に輸出する際、ISCI の基準を満たすよう求められるケースは多かった。日立製作所や三菱電機など 18 社が産業技術総合研究所などとつくる研究組合「制御システムセキュリティセンター（CSSC；Control System Security Center）」は、サイバーテロの安全基準を検討している ISCI に加盟することを発表し、CSSC から認証されれば ISCI の基準を満たすことになった。この加盟によって日本企業の製品のセキュリティ向上が期待される[83]。

一方政府では、情報セキュリティ向上のための基準、ガイドライン、監査制度等を公表している。主な取り組

[82]「サイバー防御高度に、伊藤忠テクノ、企業の耐性、総合診断、攻撃巧妙化に対応」『日本経済新聞』2013 年 8 月 22 日
[83]「電力やガスへのサイバー攻撃、日米で安全基準、インフラ輸出促進に期待」『日本経済新聞』2013 年 1 月 26 日

みは表 3 にまとめた。

「政府機関の情報セキュリティ対策のための統一基準群」は、政府機関の情報セキュリティを確保するため、政府機関のとるべき対策の統一的な枠組みを定め、各政府機関が自らの責任において対策を図るための措置を講ずることにより、政府機関全体の情報セキュリティ対策の強化・拡充を図ることを目的としている[84]。

「高度サイバー攻撃対処のためのリスク評価等のガイドライン」は主に標的型攻撃を主眼とし、関係機関と協力して標的型攻撃の攻撃手法を分析し、その特性を踏まえた攻撃者の侵入行為を妨げる設計や、運用時にログを適切に分析できるようにするための設計対策を取りまとめるとともに、政府機関において最高情報セキュリティ責任者の指揮の下、それらの対策を組織的に実施するためのガイドラインを整備している。そして本ガイドラインに基づく取組を平成 25 年 10 月から政府機関において試行し、その結果等を踏まえて、平成 26 年度から正式に実施することとしている[85]。

経済産業省は「情報セキュリティ監査制度」を設けている。これは情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与えあるいは助言を行う活動である[86]。また、「情報セキュリティガバナンス導入ガイダンス」は、経営者が情報セキュリティレベルの向上に取り組むための具体的な実装フレームワークを構築、解説したものである。

だが、民間がセキュリティ診断サービスを提供し、政府がセキュリティ基準や監査制度を実施しているこの現状を超えて、次のステップを見通す段階に来ているのではないだろうか。

上記のような官民の取り組みより一歩先に進み、一般企業や重要インフラストラクチャーのサイバーセキュリティに関して政府が「抜き打ち検査」を行い、重大な欠陥や不健全なセキュリティを発見した場合、または被害組織の過失による重大なサイバー攻撃が発生した場合、業務改善命令や業務停止命令を課すことが有効ではないだろうか。ここで参考となるのが、金融庁が行っている「金融検査」と、「食品衛生法」である。

「金融検査」とは、信用秩序の維持や預金者保護を目的に、銀行法などに基づいて金融庁が実施する検査である。金融庁の検査官が銀行等の金融機関の店舗に立ち入り、業務や資産内容などを調査し、金融機関の業務の健全性と適切性の確保、及びその金融機関が金融仲介機能を適切に果たしているかなどの検証を行う。そして本検査で法令違反や不正などが見つかった場合、金融機関に指摘の上、業務停止命令や業務改善命令などの行政処分を行うことができる。また、金融庁や各財務局の検査官が銀行等を検査するときに指針とする「金融検査マニュアル」という手引書がある。これは検査員の手引書という位置付けではあるが、同時に各金融機関はこれを踏まえて業務を自主点検し、銀行業務の健全性と適切性の確保に努めることが期待されている[87]。

「食品衛生法」では、「食品の安全性の確保のために公衆衛生の見地から必要な規制その他の措置を講ずることにより、飲食に起因する衛生上の危害の発生を防止し、もって国民の健康の保護を図ること」と目的とした法律であり、飲食物、食器、器具、容器、営業施設などに起因する衛生上の事故を防止し国民の健康を保護しようとするものである。このために様々な規制や監視が実施されており、主な規制対象は①腐敗・毒性の検査、②有害な食品添加物の検査、③各種細菌類の検査、④残留農薬の検査、⑤残留抗生物質の検査、という 5 項目である。さらに食品衛生法第 48 条は「……製造または加工を行う営業者は、その製造または加工を衛生的に管理させるため、その施設ごとに、専任の食品衛生管理者を置かなければならない」と定めている[88]。

この 2 例の仕組みと同様に、一定のセキュリティ能力

[84] 内閣官房情報セキュリティセンター『政府機関の情報セキュリティ対策のための統一規範』（http://www.nisc.go.jp/active/general/pdf/kihan24.pdf）2013 年 12 月 11 日閲覧

[85] 内閣官房情報セキュリティセンター『「高度サイバー攻撃対処のためのリスク評価等のガイドライン」について』（http://www.nisc.go.jp/active/general/risk.html）2013 年 12 月 11 日閲覧

[86] 経済産業省『経済産業省 情報セキュリティ対策ポータル』（http://www.meti.go.jp/policy/netsecurity/isaudit.html）2013 年 12 月 11 日閲覧

[87] 津田和夫ほか（2005）『金融・経済用語辞典』経済法令研究会

[88] 大鶴編（2008）pp.66-71；嘉田（2008）pp.40-42

を義務付けることにより、日本企業全体のセキュリティ向上が実現されるだろう。まず、現在ある様々な情報セキュリティ向上のための基準やガイドラインを整理・統合し、「情報セキュリティ検査マニュアル」を作成する。その抜き打ち検査をするとともに、企業はマニュアルを踏まえて自主点検して情報セキュリティの確保を図る。そして政府は企業にセキュリティ管理者の設置を義務付け、これまで課題であったセキュリティ人材の不足も、これらの実施によって企業内でのセキュリティ重要性の認識を高め、積極的なセキュリティ人材の採用に結びつくだろう。その一方で政府は第三者機関に政府機関のセキュリティ監査を委託し、自らも向上させるべきである。このような双方向のセキュリティ監査によって、日本国内のセキュリティは向上するだろう。

（2）人材育成

日本ではセキュリティ人材の深刻な不足が課題になっている。「抜き打ち検査」を実施するにしても、その前提として情報セキュリティ向上を担う人材を育成しなければならない。

民間・政府によるセキュリティ組織の設立やセキュリティ向上等の努力にも関わらず、セキュリティ人材は慢性的な人材不足に悩まされている。IPA（情報処理推進機構）の推計によると、2012 年度時点でサイバー攻撃に対応する人材は国内で 8 万人不足しているという[89]。また、国内で情報セキュリティに従事する技術者は約26 万5 千人おり、そのうち約 16 万人は再教育が必要と報告された。原因は主に 2 つあり、第 1 に教育機関の不足が挙げられる。日本の大学などには情報セキュリティの専門コースは 5 しかなく、その卒業生は年間わずか 130 人と非常に少ない。第 2 に民間企業や政府でのセキュリティ人材のキャリアパス[90]が見えないことである。セキュリティは企業の利益につながりにくいため、セキュリティ人材は評価されにくい現状がある。

また、日本ではハッカー＝犯罪者という誤った認識から人材育成が遅れていることも指摘される。海外ではハッカーの大会を開催し、技術者として優秀なハッカーをスカウトする動きが顕著になっている。アメリカでは世界最大のハッカーの祭典「デフコン」が毎年ラスベガスで開催されている。この会場にはアメリカ国土安全保障省や国防総省、軍需産業大手の幹部らの姿があり、2012 年の大会では国土安全保障省のキース・アレキサンダー長官が登場し国の安全保障への協力を呼びかけた。ロシアでは 2011 年に 2 つの国際的なハッカー会議が誕生し、優秀な発表をしたハッカーに一流企業への就職が約束されている。韓国でも政府支援の大会「コードゲート」が開催されており、優勝者には 2000 万ウォン（約 130 万円）の賞金がでる。その他中国やマレーシア、オランダでも定期的に開催されている[91]。

一方日本では、経済産業省はかつて 2003 年にデフコンと同じ実戦形式で高校生によるハッキング大会「ハッカー甲子園」を開く構想があった。しかし「国が『犯罪者』を育てるとは」と反対意見が続出し、見送られた経験がある。代わりに翌年から始まったのがウイルスの仕組みやサーバーへの侵入の仕方を教える合宿「セキュリティ&プログラミングキャンプ」であるが、犯罪に悪用される恐れがある技術は対象外になっている。しかし、遠隔操作ウイルスによる誤認逮捕事件や省庁へのサイバー攻撃が相次ぎ「正義のハッカー」の育成が急務と認識され、ハッキング大会を人材育成の場として見直す動きが出てきた。2013 年 2 月にはハッキング技術を競う初の国主催の全国大会が秋葉原で開催された。また、警察庁は NPO 法人「日本ネットワークセキュリティ協会」が主催するハッカー大会「SECCON 2013」を後援することを明らかにし、警察職員も大会に積極的に参加する考えを示した[92]。

日本もようやく「正義のハッカー」としての能力を持った技術者の育成に着手し始めたが、まだまだ十分な体制を構築するには至っていない。

セキュリティ対策サービスの NRI セキュアテクノロジ

89「育てセキュリティー人材――国内 8 万人不足、育成やコンテスト、官民動く」『日経産業新聞』2013 年 08 月 14 日

90 昇進・昇格のモデル、あるいは人材が最終的に目指すべきゴールまでの道筋のモデル、仕事における専門性を極める領域に達するまでの基本的なパターンのこと。『人材マネジメント用語集』アクティブアンドカンパニー（http://kotobank.jp/dictionary/personmanagement/）2013 年 11 月 25 日閲覧

91「[サイバーウォーズ] (6) ハッカーが守る」『読売新聞』2011 年 9 月 26 日；「[スキャナー] 米「ハッカー」重用　イベント会場で募集」『読売新聞』2012 年 8 月 5 日

92「「正義のハッカー」育成　サイバー防衛　初のコンテスト」『読売新聞』2012 年 2 月 15 日；「「正義のハッカー」全国大会　初の国主催　アキバで腕試し」『読売新聞』2013 年 2 月 4 日；「警察職員もハッカー大会に」『朝日新聞』2013 年 6 月 14 日

ーズによれば 2012 年の世界全体の情報セキュリティ人材は 287 万 2 千人であり、サイバー先進国であるアメリカは 118 万 1 千人で約 3 分の 1 以上を占めている。技術でも人材でもアメリカは世界をリードしているが、そのアメリカでも 2 万～4 万人が不足しているとされている。アメリカでは軍と民間セキュリティ人材の交流は盛んであり、最近はサイバーセキュリティ関連の任務に従事していた士官クラスの除隊者を、シマンテックやマカフィーなどアメリカのセキュリティ企業が上級幹部として積極的に雇い入れている。コンサルタントとして独立し、軍事産業や軍組織と直接契約する除隊者もいるようだ。しかし日本の場合、終身雇用制がセキュリティに関する人材や技術の流通を阻害・分断させているという指摘がある[93]。

アメリカでは情報セキュリティ企業の育成にあたって、非常にユニークな方法がとられている。その一つが軍や情報機関による積極的な企業育成である。ニューヨーク・タイムズ紙がサイバー攻撃を受けた際、その攻撃の調査を担当したマディアント会社は、アメリカ空軍の情報技術将校の OB を中心に設立・運営されている。同社は複数の投資会社から 70 億円の出資を受け、従業員 330 人で 2012 年に売上高を約 100 億円にした。アメリカでは軍や情報機関が有望な情報セキュリティのベンチャー企業に出資することによって、その企業に民間投資を呼び込む育成政策を採用している。政府の信用のお墨付きを得たベンチャー企業はその信用を背景に、政府からの出資の約 10 倍もの資金を民間から獲得するといったように、アメリカは情報セキュリティ企業を急速に成長させることに成功している。このようなベンチャーキャピタルの一つが、IN-Q-TEL という投資ファンドである。これはアメリカのインテリジェンス活動に資する最新の情報技術開発を支援、商用技術開発と諜報組織が必要とする技術のギャップを埋めることを目的に、1999 年に非営利のベンチャー投資ファンドとして国家情報会議が設立した[94]。

このように、アメリカは官民一体となって情報セキュリティ技術の開発に取り組んでいる。日本も政府が情報セキュリティ会社の支援を行い、セキュリティ企業と人材の成長を促すべきではないだろうか。

（3）外交

サイバー空間は相互接続されており国境がない。それ故に、日本政府はサイバー空間における脅威に対応するために他国との情報共有、国際的なルール作りへの積極的な参加、信頼醸成、セキュリティ研究など国境を越えた外交上のサイバー防衛を推進しなければならない。日本政府は各国と情報セキュリティ分野について活発な議論を行い、積極的なパートナーシップの構築に努めている。

アメリカとの間では、2012 年 3 月に日米両政府でサイバー攻撃の動向を監視する共通の観測網を構築することを合意した。これは互いの国で観測された攻撃情報を共有することで、いち早く対策を進めることが狙いである[95]。2013 年 5 月にはサイバー空間の脅威に関する初の対話「日米サイバー対話」を開き、サイバーテロを防ぐための包括的な協力を進めるとした共同声明を発表した。声明ではサイバーの共通課題について情報交換と協力のあり方を検討していくことを確認し、重要インフラの保護やサイバー防衛をめぐる国際的なルール作りで連携することも申し合わせた[96]。また、2013 年 10 月には日米安全保障協議委員会を開き、「サイバー防衛政策作業部会」を設けることを確認した。作業部会は日米の防衛当局間で政策のすり合わせや人材育成、2 国間の演習などを進め、連携を強める方針である[97]。

イギリスとは、2012 年 6 月に「日英サイバー協議」を開催した。サイバーセキュリティにおける国際的な規範作り、安全保障における課題、サイバー犯罪への取り組み、情報セキュリティ・システム防護、両国の取り組みの紹介や協力の可能性等について意見交換を行った[98]。

欧州委員会（EU）とは、2012 年 5 月に川端総務相と欧州連合のネーリー・クルス欧州委員（デジタル戦略担当）がブリュッセルで会談し、入手したサイバー攻撃の

[93]「米、軍出身者を積極活用、情報セキュリティー人材、自衛官、終身雇用制が壁」『日経産業新聞』2013 年 9 月 4 日
[94] 土屋ほか（2013） p.46
[95]「日米、サイバー攻撃監視網　情報共有へ　発信元やウイルス特徴」『読売新聞』2012 年 3 月 23 日
[96]「サイバー攻撃対策で初会合、日米、きょう共同声明」『日本経済新聞』2013 年 5 月 11 日
[97]「サイバー防衛で連携強化、日米外務・防衛相協議、指針改定へ」『日本経済新聞』2013 年 10 月 3 日
[98] 総務省（2013）p.300

情報を共有する枠組みを創設することで合意した[99]。同年11月には「日EUインターネット・セキュリティフォーラム」を開き、情報セキュリティに関する政策動向についての意見交換、重要インフラ防護や官民情報共有のあり方についての取り組みの共有、情報セキュリティの意識啓発活動についての意見交換が行われた[100]。

ロシアとは2013年11月に初めての外務・防衛担当閣僚級協議会合（2プラス2）を開き、「日ロサイバー安全保障協議」を立ち上げ、定例開催することに合意した[101]。

ASEAN（東南アジア諸国連合）とは、2012年10月に「第5回・ASEAN情報セキュリティ政策会議」を開催し、情報セキュリティ意識啓発に関する取り組みの推進、情報共有体制の検討など、情報セキュリティにおける一層の連携強化について合意した[102]。また、2013年9月にASEANと情報セキュリティ関係閣僚による討議を終え、共同声明を採択した。その共同声明の主な内容は、①サイバー攻撃の予知やウイルス感染に対する警告などで技術協力、②ASEANへの専門家派遣による人材育成、③重要インフラの防護、スマートフォンのセキュリティで協力促進、④サイバー攻撃対処の演習などで情報共有の仕組みを構築、などである。

インドとは2012年11月に「第1回日インド・サイバー協議」を開催し、安全保障における課題、サイバー犯罪への取り組み、情報セキュリティ・システム防護、両国の取り組みについて情報交換や協力の可能性等について意見交換を行った[103]。

また、国際連携による研究開発の強化ではサイバー攻撃やマルウェア等に関する情報を収集するネットワークを諸外国と連携して構築し、サイバー攻撃の発生を予知し即応を可能とする技術の研究開発・実証実験を実施するプロジェクト「PRACTICE（Proactive Response Against Cyber-attacks Through International Collaborative Exchange）」を進めている[104]。これまでアメリカやASEAN等の海外諸国と連携を開始している。

以上のような情報共有・研究における国際協力の推進は評価に値するだろう。各国が「サイバー攻撃」についての認識を共有し、新たな脅威についての情報を共有することにより迅速に対応することが期待される。

だが、このような他国との協力体制も実際どれほどのレベルで協力できているかは定かではない。自国の情報セキュリティの現状をそのまま国外へ話してしまえば、それは自国の弱点を他国へ伝えてしまうも同然である。それでは、逆に自らの安全保障にとってマイナスの影響を与えてしまう。日本の場合、将来敵対する見込みがなさそうな同盟国家等は心配ないが、現在領土問題を抱えている韓国や中国との情報共有は諸刃の剣にもなりかねないため、協力は慎重にするべきではないだろうか。利害関係のある2国間では協力・連携は難しい。したがって各国の利害関係を超えた国連などで議論を深めるべきだろう。

おわりに

本論文ではサイバー攻撃に対する日本のセキュリティ政策の在り方を考察した。「サイバー攻撃」という言葉が定義されておらず、危険を煽るようなメディアや研究者の論調に国際社会も引きずられているのではないかという疑いを背景に、サイバー攻撃をとりまく現状を客観的に論述してきた。その考察した結果、現段階ではサイバー攻撃元がわかりにくく犯人を特定する技術が未熟である以上、国家がサイバー攻撃に対して自衛権を発動することは早計であり、対策は民間が主体となり推進するべきであると結論付けた。そのセキュリティ向上を図るために政府は「抜き打ち検査」を実施するべきであり、国家は他国との連携を強めることも重要であると述べた。

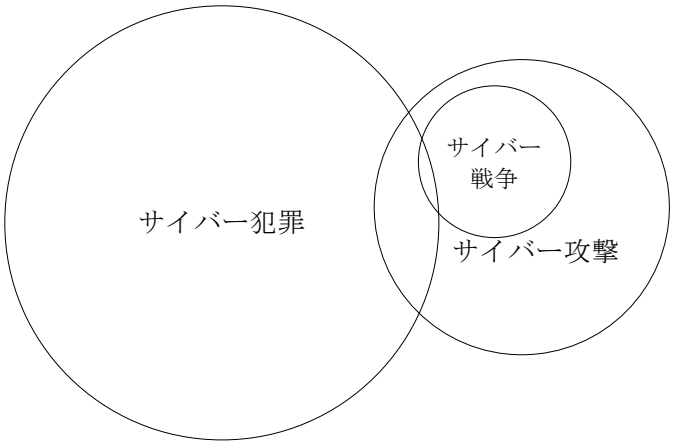
今後の課題としては、サイバー攻撃を規制する国際ルールを構築することができるのかという点である。現在

[99]「サイバー攻撃監視網　日・EUで構築合意」『読売新聞』2012年5月4日
[100] 総務省（2013）p.300
[101]「日ロ、思惑食い違い　中国への牽制／北方領土問題「2+2」安保強化で一致」『朝日新聞』2013年11月3日
[102] 総務省（2013）p.300
[103] 総務省（2013）p.300
[104] 情報セキュリティ政策会議『サイバーセキュリティ国際連携取組方針』2013年12月10日閲覧
（http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_j.pdf）

サイバー攻撃に関する国際規定が存在していない。日々変動が激しく国境が存在しないサイバー空間において、各国の様々な思惑を超えて国際ルールを構築することは難しい。また、情報セキュリティの「抜き打ち検査」を実施しようとする際、その費用は国が負担することになるが、利益と損害が分かりにくい情報セキュリティ検査について国民の賛同が果たして得られるかという問題もある。日本はまだ国民の生活に深刻な損害を与えるようなサイバー攻撃の被害に遭っておらず国民のセキュリティ意識も低いと指摘されているが、深刻なダメージを受けてからは遅いのである。我々はサイバー攻撃への国際的な自衛権を議論する前に、民間レベルでのサイバー防衛体制を整えるべきである。今後の日本のセキュリティ向上には、国民の意識改革が大きな鍵となってくるだろう。

図表

図１：サイバー諸行為の関係



出所： Oona A. Hathaway et al, 2012, *The Law of Cyber-Attack*, California Law Review, vol.100, no.4, August, p.833

表１：異なったサイバー諸行為の特徴

	サイバー行為のタイプ		
	サイバー攻撃	サイバー犯罪	サイバー戦争
非国家主体だけが関係する		○	
コンピュータ・システムの手段によって犯される刑法違反でなければならない		○	
コンピュータ・ネットワークの機能を攻撃する目的でなければならない	○		○
政治的または国家の安全目的を持っていなければならない	○		○
効果は「武力攻撃」と同等でなければならない、または武力衝突の文脈で起きなければならない。			○

出所： Oona A.Hathaway et al, 2012, *The Law of Cyber-Attack*, California Law Review, vol.100, no.4, August, p.833

表 2：日本の主なサイバー攻撃情報共有の取り組み（筆者作成）

	名称	主体
官主導	サイバーインテリジェンス共有ネットワーク	警察庁
	サイバー情報共有イニシアティブ（J-CSIP）	経済産業省と情報処理推進機構（IPA）
	テレコムアイザック官民協議会	総務省と情報通信研究機構（NICT）
	サイバーディフェンス連携協議会	防衛省
民主導	サイバーリスク情報センター	NEC、NTT、三井物産セキュリティディレクションなど 20～30 社程度
	サイバー・グリッド研究所	ラック、セキュアブレイン、アズビルセキュリティフライデーなど 10 社程度
	日本コンピュータセキュリティインシデント対応チーム協議会（日本シーサート協議会）	日立製作所、インターネットイニシアティブ、JPCERT コーディネーションセンター、ラック、NTT、ソフトバンクなど 47 社・団体

参考：「サイバー攻撃、連携で阻止、世界、ICPO が対抗拠点、国内、企業主導で情報共有」
『日経産業新聞』2013 年 11 月 29 日

表 3　日本のセキュリティ対策のための監査制度・基準・ガイドラインなど（筆者作成）

名　　称	主　　体
政府機関の情報セキュリティ対策のための統一基準群	情報セキュリティ対策会議
高度サイバー攻撃対処のためのリスク評価等のガイドライン	情報セキュリティ対策会議
情報セキュリティ監査制度	経済産業省
情報セキュリティガバナンス導入ガイダンス	経済産業省

参考文献

（著書）

相戸浩志（2007）『図解入門 よくわかる最新情報セキュリティの基本と仕組み―基礎から学ぶセキュリティリテラシー』 秀和システム

伊東寛（2012）『「第５の戦場」サイバー戦の脅威』祥伝社

猪口孝ほか編（2005）『国際政治事典』弘文堂

情報処理推進機構（2009）『情報セキュリティ教本：組織の情報セキュリティ対策実践の手引き改訂版』 実教出版

岩内亮一、藪野祐三編（2003）『国際関係用語辞典』学文社

大島邦夫、堀本勝久（2011）『2011-'12 年版［最新］パソコン・IT 用語事典』技術評論社

大鶴勝ほか編（2007）『食品加工・安全・衛生』朝倉書店

嘉田良平（2008）『改訂版 食品の安全性を考える』放送大学教育振興会

加藤朗（1993）『現代戦争論：ポストモダンの紛争 LIC』中央公論社

加藤秀治郎、渡邊啓貴編（2002）『国際政治の基礎知識』芦書房

リチャード・クラーク、ネイク・ロバート（2011）『核を超える脅威 世界サイバー戦争 見えない軍拡が始まった』（北川 知子、峯村 利哉訳）徳間書店

小寺彰ほか編（2004）『講義国際法』有斐閣

秀和システム第一出版編集部編著（2011）『最新標準パソコン用語事典〈2011-2012 年版〉』秀和システム

ジョセフ・ナイ、ウェルチ・デイヴィッド著、田中明彦、村田晃嗣訳（2011）『国際紛争：理論と歴史　原書第８版』有斐閣

高橋和之ほか編 （2010）『インターネットと法 第４版』有斐閣

谷口長世（2012）『サイバー時代の戦争』岩波書店

津田和夫ほか（2005）『金融・経済用語辞典』経済法令研究会

土屋大洋（2012）『サイバー・テロ 日米 vs.中国』文藝春秋

塚越健司（2012）『ハクティビズムとは何か ハッカーと社会運動』ソフトバンククリエイティブ

山本草二（1994）『国際法 新版』有斐閣

松井芳郎（2011）『国際法から世界を見る：市民のための国際法入門 第３版』東信堂

（論文）

朝長秀誠、渡邉浩一郎（2012）「サイバー・セキュリティーの現状：サイバー攻撃の動向とその対策に向けて」『Provision』73 号 pp. 26-31

リン・J・ウィリアム（2011）「高度化する脅威と進化するサイバー戦略：なぜ官民協調型サイバー防衛が必要か」『Foreign affairs repot』第 11 号 pp.102-107

岡垣知子（2006）「『先制』と『予防』の間――ブッシュ政権の国家安全保障戦略――」『防衛研究所紀要』第９巻第１号 pp.15-23

小林偉昭ほか（2012）「サイバー攻撃の脅威とその対策」『電気学会誌』132 巻６号 pp.344-348

中谷和弘（2013）「サイバー攻撃と国際法の対応」『ジュリスト』1454 号 pp.58-63

名和和男（2012）「サイバー攻撃から組織・企業を守る」『電気学会誌』132 巻６号 pp.349-353

ネイク・ロバート（2011）「インターネットのジレンマ――セキュリティと相互運用性をいかに両立させるか」『Foreign affairs report』２号 pp.82-92

春名幹男（2011）「米国の新サイバー戦略」『海外事情』59 巻７・８号 pp.109-124

バレリアーノ・ブランドン、マネス・ライアン（2013）「サイバー戦争の虚構と現実」『Foreign affairs report』１号 pp.91-96

ヨハイ・ベンクラー（2012）「アノニマスの活動はテロか抗議行動か：サイバー空間と抗議行動」『Foreign affairs repot』５号 pp.28-87

（政府刊行物）

情報セキュリティ政策会議『サイバーセキュリティ 2013』（http://www.nisc.go.jp/active/kihon/pdf/cs2013.pdf）2013 年 12 月 23 日閲覧

情報セキュリティ政策会議『サイバーセキュリティ　国際連携取組方針～j-initiative for Cybersecurity～』（http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_j.pdf）2013 年 12 月 23 日閲覧

情報セキュリティ政策会議『サイバーセキュリティ戦略～世界を率先する強靭で活力あるサイバー空間を目指して～』（http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf）2013 年 12 月 23 日閲覧

総務省（2012）『情報通信白書　平成 24 年版』

総務省（2013）『情報通信白書　平成 25 年版』

防衛省（2012）『日本の防衛　平成 24 年版――防衛白書』
防衛省（2013）『日本の防衛　平成 25 年版――防衛白書』

（外国語文献）
CCD COE（2013）『The Tallinn Manual』（http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381）2013 年 12 月 23 日閲覧
Heather Harrison Dinniss（2012）,*Cyber warfare and the laws of war*, Cambridge University Press
Oona A.Hathaway et al（2012）, *The Law of Cyber-Attack*, California Law Review, vol.100, no.4, August, pp.817-885.

（ネット情報）
土屋大洋（2013a）「第 8 章　米国におけるサイバーセキュリティ政策」『米国内政と外交における新展開』日本国際問題研究所（http://www2.jiia.or.jp/pdf/resarch/H24_US/H24_US.php）2013 年 12 月 20 日閲覧 pp.133-146
土屋大洋（2013b）「第 5 章　第四と第五の作戦空間の登場：宇宙とサイバーの交差」『平成 24 年度外務省委託事業『宇宙に関する各国の外交政策』についての調査研究　提言・報告書』（http://www.jfir.or.jp/j/activities/reseach/pdf/59.pdf）2013 年 12 月 16 日閲覧
土屋大洋ほか著（2013）「サイバー攻撃の実態と防衛　報告書」21 世紀政策研究所（http://www.21ppi.org/pdf/thesis/130611.pdf）2013 年 12 月 23 日閲覧
François Paget（2012）「ハクティビズム　政治的発言の新たな媒体となったサイバー空間」「McAfee セキュリティ研究レポート」（http://b2b-download.mcafee.com/products/japan/pdf/threatreport/wp_hacktivism.pdf）2012 年 12 月 20 日閲覧
防衛省（2012）「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」（http://www.mod.go.jp/j/approach/others/security/cyber_security_sisin.html）2013 年 12 月 3 日閲覧
McAfee（2011）「サイバー犯罪の 10 年間」『McAfee セキュリティ研究レポート』（http://b2b-download.mcafee.com/products/japan/pdf/threatreport/1102_Decade_of_Cybercrime.pdf）2013 年 12 月 15 日閲覧
McAfee（2012）「サイバー防衛報告書『サイバーセキュリティ：世界ルールの主たる争点』概要」『McAfee セキュリティ研究レポート』（http://b2b-download.mcafee.com/products/japan/pdf/threatreport/Report_CyberDefense.pdf）2013 年 12 月 25 日閲覧
McAfee（2013）「In the Dark 重要産業が直面するサイバー攻撃」『McAfee セキュリティ研究レポート』（http://b2b-download.mcafee.com/products/japan/pdf/threatreport/RPT_CIP_21900rpt_A4_1301.pdf）2013 年 12 月 20 日閲覧